Hepting et al v. AT&T Corp. et al Doc. 349

Laurence F. Pulgram (CSB No. 115163)
lpulgram@fenwick.com
Candace Morey (CSB No. 233081)
cmorey@fenwick.com
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350

Ann Brick (CSB No. 65296)
abrick@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (4150 255-8437

Attorneys for Plaintiffs in
Dennis P. Riordan, *et al.*

Barry R. Himmelstein (CSB No. 157736)
bhimmelstein@lchb.com
LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
275 Battery Street, 30th Floor
San Francisco, CA 94111-3339
Telephone: 415-956-1000
Facsimile: 415-956-1008

Interim Class Counsel for MCI Class

Vincent I. Parrett (CSB No. 237563)
vparrett@motleyrice.com
MOTLEY RICE LLC
28 Bridgeside Boulevard
P. O. Box 1792
Mount Pleasant, SC 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9440

Interim Class Counsel for
Verizon Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE:

NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION,

This Document Relates To:

(1) All Class Actions Against MCI and Verizon Defendants in the Master MCI and Verizon Consolidated Complaint, Dkt. 125;
(2) *Bready v. Verizon Maryland* (06-6313);
(3) *Chulsky v. Cellco Partnership & Verizon Communications Inc.* (06-6570); and
(4) *Riordan v. Verizon Communications Inc.* (06-3574)

MDL No. 06-1791 VRW

PLAINTIFFS' JOINT OPPOSITION TO MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT BY THE UNITED STATES OF AMERICA AND TO STATE SECRETS AND RELATED ARGUMENTS IN VERIZON'S MOTION TO DISMISS

Date: August 30, 2007
Time: 2:00 p.m.
Courtroom: 6, 17th Floor
Judge: Hon. Vaughn R. Walker

Dockets.Justia.com

Jennifer L. Kelly (CSB No. 193416)
jkelly@fenwick.com
Aaron K. Perzanowski (CSB No. 244921)
aperzanowski@fenwick.com
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350

Peter J. Eliasberg (CSB No. 189110)
peliasberg@aclu-sc.org
Peter Bibring (CSB No. 223981)
pbibring@aclu-sc.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA
1616 Beverly Boulevard
Los Angeles, CA 90026
Telephone: (213) 977-9500
Facsimile: (213) 250-3919

Nicole A. Ozer (CSB No. 228643)
nozer@aclunc.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (4150 255-8437

Attorneys for Plaintiffs in
Dennis P. Riordan, *et al.*

Elizabeth Cabraser (CSB No. 83151)
ecabraser@lchb.com
Eric B. Fastiff (CSB No. 182260)
efastiff@lchb.com
Allison Elgart (CSB No. 241901)
aelgart@lchb.com
LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
275 Battery Street, 30th Floor
San Francisco, CA 94111-3339
Telephone: 415-956-1000
Facsimile: 415-956-1008 (fax)

Interim Class Counsel for MCI Class

Joshua Graeme Whitaker
(Appearing pursuant to MDL Rule 1.4 [U.S. Dist. Ct. for the Dist. of Md. Bar No. 16457])
joshuawhitaker@griffinwhitaker.com
Edward Nelson Griffin
(Appearing pursuant to MDL Rule 1.4 [U.S. Dist. Ct. for the Dist. of Md. Bar No. 16435])
edwardgriffin@griffinwhitaker.com
GRIFFIN WHITAKER LLP
8730 Georgia Avenue Suite LL100
Silver Spring, MD 20910
Telephone: (301) 587-3345
Facsimile: (888) 367-0383

Attorneys for Plaintiffs
Christopher Bready, *et al.*

Ronald L. Motley
rmotley@motleyrice.com
Jodi W. Flowers
jflowers@motleyrice.com
Don Migliori
dmigliori@motleyrice.com
Justin B. Kaplan
jkaplan@motleyrice.com
MOTLEY RICE LLC
28 Bridgeside Boulevard
P. O. Box 1792
Mount Pleasant, SC 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9440

Interim Class Counsel for
Verizon Class

David H. Sternlieb
dsternlieb@shapirosternlieb.com
Gary S. Shapiro
gshapiro@shapirosternlieb.com
(Appearing pursuant to MDL Rule 1.4) (U.S. Dist. Ct. for the Dist. of N.J.)
SHAPIRO & STERNLIEB, LLC
Attorneys At Law
800 Tennent Road
Manalapan, New Jersey 07726
Telephone: (732) 617-8050
Facsimile: (732) 617-8060

Counsel for
Plaintiffs Glen Chulsky, *et al.*

TABLE OF CONTENTS

Page(s)

ISSUES TO BE DECIDED xi

INTRODUCTION 1

THE FACTUAL BACKGROUND 2

A. This Court Has Already Rightly Concluded that Evidence Confirms the Existence of the NSA Content Surveillance Program 2

B. Reliable Public Information Unequivocally Confirms the Existence of an NSA Program for Collecting Customer Call Records 4

1. The Executive Branch Has Confirmed a Call Records Program Exists 5

2. Members of Congress Fully Briefed on the NSA Programs Have Acknowledged the Call Records Program 5

3. Verizon, as Well as Qwest, Has Confirmed the Call Records Program. 8

C. The Facts Regarding Verizon's and MCI's Participation in the Content and Records Programs Is Not a Secret 9

D. Verizon's and MCI's Turnover of Call Records to the Government Is a Public Fact Well Known to Potential Terrorists 11

ANALYSIS 14

I. THIS COURT IN *HEPTING* APPLIED THE PROPER STANDARDS FOR ANALYSIS OF THE STATE SECRETS PRIVILEGE 14

A. The Judiciary, Not the Executive, Determines the Applicability and Effect of the State Secrets Privilege 14

B. The Court Must First Find the Information to be Secret Before Reasonable Harm from Disclosure Could Become Relevant 16

1. Information Publicly Disclosed by Reliable Sources Is Not Secret 17

2. The Government's Claim that It Has Not Intentionally Waived the Privilege Cannot Cloak Non-Secret Information 18

3. Truly Secret Information Is Subject to the Privilege Only if Disclosure Threatens National Security 19

FENWICK & WEST LLP
ATTORNEYS AT LAW
SAN FRANCISCO

TABLE OF CONTENTS
(continued)

Page(s)

II. "THE VERY SUBJECT MATTER" OF THIS LITIGATION IS NOT A SECRET; ACCORDINGLY THE GOVERNMENT'S ASSERTION OF THE STATE SECRETS PRIVILEGE CANNOT BAR ALL CLAIMS AT THE OUTSET 20

A. Dismissal is a Draconian Remedy Unsupported by Precedent Here 20

B. The Public Record Reveals the Existence of the Programs and the Participation of MCI and Verizon 23

1. The Existence of the Content Monitoring Program Is Not Secret. 23

2. The Existence of the Call Records Program Is Not Subject to the State Secrets Privilege 24

a. Executive Disclosures Reveal the Existence of the Call Records Program 24

b. Congressional Disclosures Reveal the Existence of the Call Records Program 25

c. Party Disclosures Reveal the Existence of the Call Records Program 26

3. Participation by MCI and Verizon in Both the Content and Records Program Is Not Secret 27

a. The Participation of Verizon and MCI in the Content Surveillance Program Is Not Secret 27

b. Participation by Verizon's MCI Subsidiary in the Call Records Program Is Not Secret 28

c. Verizon's Direct Participation in the Call Records Program Is Not Secret 29

d. Testing Verizon's Participation Through More Formal Means Will Not Harm National Security 29

III. THESE CASES MAY NOT BE DISMISSED AT THE PLEADING STAGE BASED ON THE HYPOTHESIS THAT PLAINTIFFS MAY BE UNABLE TO ESTABLISH A *PRIMA FACIE* CASE, THAT DEFENSES MAY BE UNAVAILABLE, OR THAT PLAINTIFFS MAY BE UNABLE TO PROVE STANDING 31

A. Mere Speculation That Evidence Needed to Establish a *Prima Facie* Case or Defense May Be Unavailable Cannot Support Dismissal 31

TABLE OF CONTENTS
(continued)

Page(s)

B. The Government's Hypothesized Lack of Standing Provides No Basis for Dismissal on the Pleadings 33

1. The Government's Motion For Summary Judgment is Premature 34

a. It Is Not Appropriate to Address Standing Before a Ruling on the Government's Assertion that the Very Subject Matter of this Litigation is a State Secret 34

b. Plaintiffs Are Not Required to *Prove* Standing Before Discovery 35

c. Neither *Halkin* Nor *Ellsberg* "Foreclose Litigation" Before Discovery 36

2. Proof of the Existence of the Content and Records Programs Establishes Standing 37

a. Establishing that the Dragnet Programs Exist Establishes Plaintiffs' Standing 38

b. Plaintiffs Can Establish Standing to Sue for Damages for Past Injuries and to Enjoin Probable Future Injuries. 39

3. Plaintiffs Can Establish Standing Via In Camera Proceedings 41

IV. THE *TOTTEN/TENET* BAR DOES NOT APPLY 42

A. *Totten/Tenet* Only Bars Spies from Suing the Government to Enforce Their Espionage Contracts 43

B. Verizon's Public and Admitted Assistance to Government Surveillance Is Not a "Secret" that the *Totten/Tenet* Bar Protects 45

V. STATUTORY PRIVILEGES DO NOT BAR DISCOVERY INTO VERIZON'S AND MCI'S ACTIONS, AND IN ANY EVENT, DISMISSAL AT THIS STAGE WOULD NOT BE WARRANTED 46

VI. EVEN IF THE SUBJECT MATTER WERE SECRET, THE EXECUTIVE CANNOT IGNORE EXPLICIT PROCEDURES CONGRESS ESTABLISHED FOR REVIEW OF THE REQUESTED INFORMATION. 49

A. Congress May Properly Limit Executive Authority by Statute 49

B. FISA's Well-Defined Procedures Govern Secret Information Relating to Electronic Surveillance 50

TABLE OF CONTENTS
(continued)

Page(s)

C. Dismissal on the Pleadings Is Impermissible Under § 1806(f) 53

CONCLUSION 54

TABLE OF AUTHORITIES

Page(s)

CASES

ACLU v. NSA,
438 F. Supp. 2d 754 (E.D. Mich. 2006) 18

ACLU Found. of Southern Cal. v. Barr,
952 F.2d 457 (D.C. Cir. 1991) 53

ACLU v. Brown,
619 F.2d 1170 (7th Cir. 1980) (*en banc*) 17

Al-Haramain Islamic Found. v. Bush,
451 F. Supp. 2d 1215 (D. Or. 2006) .... passim

Am. Petroleum Inst. v. EPA,
216 F.3d 50 (D.C. Cir. 2000) 40

American Library Ass'n v. FCC,
401 F.3d 489 (D.C. Cir. 2005) 40

Baker v. Carr,
369 U.S. 186 (1962) 41

Bareford v. Gen. Dynamics Corp.,
973 F.2d 1138 (5th Cir. 1992) 31

Barker v. Wingo,
407 U.S. 514 (1972) 19

Baur v. Veneman,
352 F.3d 625 (2d Cir. 2003) 39, 40

Capital Cities Media, Inc. v. Toole,
463 U.S. 1303 (1983) 17

Central Delta Water Agency v. United States,
306 F.3d 938 (9th Cir. 2002) 38, 40

CIA v. Sims,
471 U.S. 159 (1985) 48

Clift v. United States,
597 F.2d 826 (2d Cir. 1979) 21, 31

Clift v. United States,
808 F. Supp. 101 (D. Conn. 1991) 21

Clinton v. New York,
524 U.S. 417 (1998) 40

Covington v. Jefferson County,
358 F.3d 626 (9th Cir. 2004) 40

Dept. of Commerce v. U.S. House of Reps.,
525 U.S. 316 (1999) 41

Dickerson v. United States,
530 U.S. 428 (2000) 50

FENWICK & WEST LLP
ATTORNEYS AT LAW
SAN FRANCISCO

TABLE OF AUTHORITIES
(continued)

Page(s)

Does I through XXIII v. Advanced Textile Corp.,
214 F.3d 1058 (9th Cir. 2000).. 42

Edmond v. United States,
520 U.S. 651 (1997).. 22, 47

Edmonds v. DOJ,
323 F. Supp. 2d 65 (D.D.C. 2004),
aff'd, 161 Fed. Appx. 6 (D.C. Cir. 2005).. 22

Ellsberg v. Mitchell,
709 F.2d 51 (D.C. Cir. 1983).. passim

El-Masri v. United States,
479 F.3d 296 (4th Cir. 2007).. 17, 21, 22, 45

Farnsworth Cannon, Inc. v. Grimes,
635 F.2d 268 (4th Cir. 1980),
rev'd en banc on other grounds,
1980 U.S. App. LEXIS 11406 (4th Cir. 1980).. 14

FDA v. Brown & Williamson Tobacco Corp.,
529 U.S. 120 (2000).. 47

Fitzgerald v. Penthouse Int'l, Ltd.,
776 F.2d 1236 (4th Cir. 1985).. 21

Fitzgibbon v. CIA,
911 F.2d 755 (D.C. Cir. 1990).. 48

Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.,
204 F.3d 149 (4th Cir. 2000).. 40

Halkin v. Helms,
598 F.2d 1 (D.C. Cir. 1978).. 25, 26, 36, 37

Halkin v. Helms,
690 F.2d 977 (D.C. Cir. 1982).. 15, 36, 37, 38

Hall v. Norton,
266 F.3d 969 (9th Cir. 2001).. 40

Halpern v. United States,
258 F.2d 36 (2d Cir. 1958).. 41, 50, 52

Hamdan v. Rumsfeld,
126 S. Ct. 2749 (2006).. 15, 49

Hamdi v. Rumsfeld,
542 U.S. 507(2004).. 16, 50

Helling v. McKinney,
509 U.S. 25 (1993).. 39

Hepting v. AT&T Corp.,
439 F. Supp. 2d 974 (N.D. Cal. 2006).. passim

Home Bldg. & Loan Ass'n v. Blaisdell,
290 U.S. 398 (1934).. 50

TABLE OF AUTHORITIES
(continued)

Page(s)

In re NSA Telcoms. Records Litig.,
483 F. Supp. 2d 934 (N.D. Cal. 2007) 23

In re United States,
872 F.2d 472 (D.C. Cir. 1989) 15, 16, 19, 21

Int'l Bhd. of Teamsters v. TSA,
429 F.3d 1130 (D.C. Cir. 2005) 40

Jabara v. Kelley,
75 F.R.D. 475 (E.D. Mich. 1977) 18, 25

Johnson v. Zerbst,
304 U.S. 458 (1938) 19

Kasza v. Browner,
133 F.3d 1159 (9th Cir. 1998) .... passim

Loral Corp. v. McDonnell Douglas Corp.,
558 F.2d 1130 (2d Cir. 1977) 41

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 35

Maxwell v. First Nat'l Bank,
143 F.R.D. 590 (D. Md. 1991),
aff'd, 998 F.2d 1009 (4th Cir. 1993) 22

McGhehee v. Casey,
718 F.2d 1137 (D.C. Cir. 1983) 17

Mistretta v. United States,
488 U.S. 361 (1989) 49

Myers v. United States,
272 U.S. 52 (1926) 49

Nat'l Coal. for Students with Disabilities Educ. and Legal Defense Fund v. Scales,
150 F. Supp. 2d 845 (D. Md. 2001) 35

Pengate Handling Sys. v. Westchester Surplus Lines Ins. Co.,
No. 1:06-CV-0993, 2007 U.S. Dist. LEXIS 13303
(M.D. Pa. Feb. 27, 2007) 19

People for the Am. Way Found. v. NSA Cent. Sec. Serv.
462 F. Supp. 2d 21 (D.D.C. 2006) 48

Public Citizen v. U.S. DOJ,
491 U.S. 440 (1989) 15

Salisbury v. United States,
690 F.2d 966 (D.C. Cir. 1982) 26

Scanlon v. Bricklayers & Allied Craftworkers, Local No. 3,
No. 05-CV-628A(F), 2007 U.S. Dist. LEXIS 29798
(W.D.N.Y. Apr. 23, 2007) 19

Sedco Int'l, S. A. v. Cory,
683 F.2d 1201 (8th Cir. 1982) 19

TABLE OF AUTHORITIES
(continued)

Page(s)

Snepp v. United States, 444 U.S. 507 (1980) ... 48

Spock v. United States, 464 F. Supp. 510 (S.D.N.Y. 1978) ... 18, 41

Sterling v. Tenet, 416 F.3d 338, 347 (4th Cir. 2005), *cert. denied*, 126 S. Ct. 1052 (2006) ... 22

Tenet v. Doe, 544 U.S. 1 (2005) ... 42-45, 50

Terkel v. AT&T Corp., 441 F. Supp. 2d 899 (N.D. Ill. 2006) ... passim

Totten v. United States, 92 U.S. 105 (1875) ... 42-46, 50

United States v. Adams, 473 F. Supp. 2d 108 (D. Me. 2006) ... 27

United States v. Fell, 360 F.3d 135 (2d Cir. 2004) ... 50

United States v. Nixon, 418 U.S. 683 (1974) ... 49

United States v. Reynolds, 345 U.S. 1 (1953) ... passim

Upjohn Co. v. United States, 449 U.S. 383 (1981) ... 19

Village of Arlington Heights v. Metro. Housing Dev. Corp., 429 U.S. 252 (1977) ... 41

Walters v. Edgar, 163 F.3d 430 (7th Cir. 1998) ... 40

Weinberger v. Catholic Action of Hawaii/Peace Educ. Project, 454 U.S. 139 (1981) ... 30, 44, 45

Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S, 579 (1952) ... 49, 51, 54

Zuckerbraun v. Gen. Dynamics Corp., 935 F.2d 544 (2d Cir. 1991) ... 22

STATUTES

18 U.S.C. § 2511(2)(f) ... 51

18 U.S.C. § 2520(a) ... 51

18 U.S.C. § 2707(a) ... 51

18 U.S.C. § 2709 ... 13

18 U.S.C. § 2709(d) ... 13

TABLE OF AUTHORITIES
(continued)

Page(s)

47 U.S.C. § 605(e)(3)(A) 51
50 U.S.C. § 402 47
50 U.S.C. § 403-1(i)(1) 47
50 U.S.C. § 1801(f)(1) 53
50 U.S.C. § 1801(f)(2) 52
50 U.S.C. § 1806(f) .... passim
50 U.S.C. § 1809 51
50 U.S.C. § 1810(a)(I) 51
50 U.S.C. § 1845(f) 47
50 U.S.C. § 2511(2)(a)(ii)(B) 47

RULES

Fed. R. Civ. P. 56 37
Fed. R. Civ. P. 56(f) 33, 35
Pub. L. No. 95-511, 92 Stat. 1783, § 201 (1978) 51

OTHER AUTHORITIES

1A. Conte & H. Newberg, *Newberg on Class Actions* § 2.5 (4th ed. 2002) 41
26 Wright & Graham, *Fed. Prac. & Proc.* § 5665 .... 19, 27
S. Rep. No. 94-755 (II) 51
S. Rep. No. 95-604 (I) 51, 52, 53

ISSUES TO BE DECIDED

1. Whether, under the appropriate standard of review and method of analysis as articulated in *Hepting v. AT&T Corp*, 439 F. Supp. 2d 974 (N.D. Cal. 2006), Plaintiffs' claims are barred by the Government's assertion of the state secrets privilege.

2. Whether reliable public disclosures confirming or denying Verizon's and MCI's participation in the Executive's warrantless communications content and call records surveillance programs render "the very subject matter" of the cases non-secret.

3. Whether facts alleged by Plaintiffs are sufficient at this initial stage of the case to establish standing.

4. Whether the *Totten/Tenet* categorical bar applies where Plaintiffs do not seek to enforce terms of their own secret espionage relationship with the Government.

5. Whether statutory privileges that only address information disclosures by the Government are a basis for dismissing these cases their entirety.

6. Whether procedures prescribed by Congress in the Foreign Intelligence Surveillance Act, 18 U.S.C. § 1806(f), for challenges to foreign intelligence surveillance activities mandate the procedure for analysis of Defendants' challenged electronic surveillance activity, notwithstanding the Executive's efforts to preclude inquiry at the outset.

INTRODUCTION

In their Motions to Dismiss on state secrets grounds, the Government and Verizon Communications, Inc. ("Verizon")[1] doggedly dispute the analytical framework in *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006). They challenge, among other things, the Court's findings as to the threshold showing necessary for application of the state secrets privilege, the impropriety of dismissal prior to discovery, the reach of the *Totten* doctrine, the impact of any privilege on Plaintiffs' ability to establish standing and the application of statutory privileges. Although these arguments are no more persuasive the second time around, the Government's effort to rehash them is not surprising. Unless the Government succeeds in displacing this Court's reasoned analysis in *Hepting*, the Motion to Dismiss is doomed. The Government therefore urges the Court to abandon its conclusions in *Hepting* and adopt the Executive's preferred approach—one that transgresses the line separating judicial deference from subservience.

The Government fails to identify a single fact in the Verizon lawsuits that would lead to a more favorable outcome for it under the analysis the Court employed in *Hepting*. Indeed, it does not even try. And while there *are* significant factual differences between *Hepting* and the present cases, they support this Court's analysis and lead to an even more favorable result for Plaintiffs. The challenged content surveillance program has become no more secret over the past year. By contrast, any shroud of uncertainty cloaking the call records program has since lifted. As this Court predicted, disclosures have continued, including from numerous members of Congress fully briefed on the program and Verizon itself, confirming that an NSA program exists to amass and analyze telephone calling records. These disclosures provide ample factual certainty to overcome this Court's hesitancy to allow discovery on such claims a year ago. *See* 439 F. Supp. 2d at 997-98 (suggesting that plaintiffs "can request that the court revisit this issue" if future "disclosures [] make [the records] program's existence or non-existence no longer a secret").

The same analysis that demanded rejection of the Government's efforts to scuttle *Hepting* at the pleading stage militates even more strongly against such a harsh and aberrant result here and warrants discovery on both the call records and content surveillance programs.

---

[1] This brief also responds to the state secrets arguments Verizon makes in support of its Motion to Dismiss the Master Consolidated Complaint ("MCC") (Docket No. 273).

THE FACTUAL BACKGROUND

It is now indisputable that telecommunications companies have been helping the NSA intercept telephone calls as well as providing tens of millions of call records to the NSA. In the year since this Court issued its decision in *Hepting*, new public disclosures have continued to pile up verifying the existence and nature of both, including:

- An ever growing roster of Congresspersons have, primarily in attempts to defend the program, acknowledged the turnover of call records;
- Verizon as well as Qwest Communications International, Inc. ("Qwest") have now directly acknowledged the Government's requests for their participation in the call records program; and
- Verizon as well as Department of Justice ("DOJ") officials have acknowledged Verizon's cooperation in turning over call records in response to National Security Letters—at times without the required legal authorization of an NSL.

These facts are known to anyone who cares to look, whether he bids our nation ill or good. Verizon's and MCI's assistance in the unlawful surveillance therefore cannot be cloaked as a "state secret" immune from judicial scrutiny.

A. This Court Has Already Rightly Concluded that Evidence Confirms the Existence of the NSA Content Surveillance Program.

This Court has previously found that because "significant amounts of information about the government's monitoring of communication content and AT&T's intelligence relationship with the Government are already nonclassified or in the public record," the existence of the NSA's warrantless program of intercepting and monitoring communications content is "hardly a secret." *Hepting*, 439 F. Supp. 2d at 994; *see also, id.* at 991-92 ("AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content."). President Bush admitted the existence of the NSA's communications content monitoring program in his December 17, 2005 radio address, stating that he "authorized the National Security Agency . . . to intercept the international communications of people with known links to Al Qaeda and related terrorist organizations." Ex. A at 2 (President's Radio

Address).[2] Likewise, Attorney General Alberto Gonzales subsequently confirmed that the program involved "intercepts of contents of communications." Ex. B at 1 (Alberto Gonzales Press Briefing, Dec. 19, 2005). The Government thereby revealed "the general contours" of NSA's program that "monitor[s] communication content [and] operates without warrants." *Hepting*, 439 F. Supp. 2d at 992-93. Plaintiffs allege that the NSA's surveillance program is far broader that the limited interceptions of international calls than the Government has disclosed.

More recently, the dramatic Congressional testimony of Deputy Attorney General James Comey has exposed new facts about the illegal nature of the Administration's surveillance activities. Ex. C (Sen. Judiciary Comm. Hearing, May 15, 2007). Comey, who was chief deputy to John Ashcroft, testified about the March 2004 efforts of then White House Counsel Alberto Gonzales and Chief of Staff Andrew Card to strong-arm Ashcroft into reauthorizing a secret program from his hospital bed. *Id*. at 8-9. Both Ashcroft and Comey, who was Acting Attorney General at that time, agreed that they could *not* attest to the program's legality and *refused* to sign the reauthorization. *Id*. at 8-9. The White House nonetheless reauthorized the program, *id*. at 12, 21-22, allowing its operation for weeks without legal certification from the DOJ. Ex. D at 4 (Comey Written Response). Only under threats of resignation by Comey, FBI Director Robert Mueller and others did the White House approve changes to bring the program within the strictures demanded by the Administration's own appointees. *See* Ex. C at 12-14.

Although Mr. Comey has not identified which classified program was up for reapproval, it was a program for intelligence surveillance of communications. Yet, Attorney General Gonzales has testified that there was never any "serious disagreement" within the DOJ about the legality of what the President describes as the "TSP"—warrantless tapping into *international* calls of known Al Qaeda operatives. *See* Ex. E at 9-10 (Sen. Judiciary Comm. Hearing, Feb. 6, 2006) (Comey's reservations were about other "operational capabilities," but "did not deal with the program that I'm here testifying about today,"—the TSP). Thus, the program Comey testified about was likely an aspect of the dragnet surveillance of telecommunications content, or the turnover of call records. In any event, full facts about the program will likely come to light during this litigation. Two days ago, by a 13-3 vote, the Senate Judiciary Committee authorized subpoenas to the DOJ and White House for documents related to legal justifications for the NSA programs. Ex. F at 1. The House Intelligence Committee intends to hear private testimony next month from Attorney General Gonzales, FBI Director Mueller, and CIA Director Michael Hayden on the programs, with the goal of holding public hearings in the fall. *Id*. The House Judiciary Committee has also asked Comey to clarify what programs were at issue. Ex. G at 2 (Conyer's Letter, May 17, 2007).

---

[2] All citations to Exhibits herein are exhibits to the Declaration of Candace J. Morey In Support of Plaintiffs' Joint Opposition to the Motions to Dismiss by the United States and Verizon.

B. Reliable Public Information Unequivocally Confirms the Existence of an NSA Program for Collecting Customer Call Records.

One year ago this Court was "hesitant to conclude that the existence or non-existence of the communication records program necessarily constitutes a state secret." *Hepting*, 439 F. Supp. 2d at 997. The Court need hesitate no longer. As predicted, substantial public disclosures have since confirmed the existence and revealed the general contours of a program highlighted by a May 11, 2006, *USA Today* article about the provision of telephone calling records of tens of millions of Americans to the NSA. Ex. H at 1.[3]

The President has publicly acknowledged the call records program in an attempt to justify its legality. So have members of Congress who were fully briefed on the program and attempted to defend it as gathering mere "business records." As more members of Congress were briefed, the number of confirmations grew, and by May 2007, nine fully briefed members of Congress had publicly confirmed the program's existence. Finally, in April 2007, Verizon joined Qwest in publicly confirming that the NSA asked for its customers' call records. Individually and collectively, these sources confirm that the NSA was not only intercepting calls, but was also amassing a database of personal call records.

---

[3] The *USA Today* article called attention to reports that the NSA "besides actually eavesdropping on specific conversations, [has] combed through large volumes of phone and internet traffic," in a "large data-mining operation." Ex. I at 1 (N.Y. Times, Dec. 24, 2005). *See also, e.g.*, Ex. J at 1 (New Yorker, May 29, 2006) (Seymour Hersh reporting that "[a] security consultant working with a major telecommunications carrier told me that his client set up a top-secret high-speed circuit between its main computer complex and . . . the site of a government-intelligence computer center," providing "total access to all the data"); Ex. K at 1 (N.Y. Times, Jan. 17, 2006); Ex. L at 1 (Nat'l. J., Jan. 20, 2006); Ex. M at 1 (Wash. Post, Feb. 5, 2006).

1. The Executive Branch Has Confirmed a Call Records Program Exists.

The Administration jumped to defend the legality of the call records program revealed by the original *USA Today* article—a defense that only confirmed the program's existence. Indeed, just four days later, President Bush's response to a question about the call records database acknowledged its existence, while also arguing that Congressional briefing about the program should allay concerns. He spoke during a May 15, 2006 press conference:

> Q: Thank you, Mr. President. Mr. President, you've said that the government is not trolling through the lives of innocent Americans, ***but why shouldn't ordinary people feel that their privacy is invaded by the NSA compiling a list of their telephone calls?***
>
> PRESIDENT BUSH: What I have told the American people is, we'll protect them against an al Qaeda attack, and we'll do so within the law. . . .
>
> ***The program he's asking about*** is one that has been fully briefed to members of the United States Congress, in both political parties. They are very aware of what is taking place. . . .

Ex. N at 2 (White House Press Conference). This colloquy did ***not*** address content interception. The President's answer was in direct response to a question about "the NSA compiling a list of [ordinary people's] telephone calls" and his reference to "the program . . . fully briefed" to Congress can only be taken as confirmation of the call records program.

A week later, Attorney General Gonzales defended the program in response to a question about the collection of "telephone detail records from the phone companies." In comments not submitted before the *Hepting* decision, he said that "what was in the *USA Today* story did relate to business records" and that "[t]here are a number of legal ways, of course, that the government can have access to business records." Ex. O at 6-7 (Press Conference, May 23, 2006).

2. Members of Congress Fully Briefed on the NSA Programs Have Acknowledged the Call Records Program.

The efforts to circle the wagons and defend the call records program did not stop at the Executive Branch. In the weeks after *USA Today* broke the story, several Senators—whom the Administration admits have been fully briefed on *all* NSA programs—made on-the-record defenses of the program. These defenses acknowledged its existence (if not its details) in sounding the same "business records" defense as the Attorney General.

For example, Senator Pat Roberts characterized the collection of private customer call records as "business records" of the telecommunications companies, in an attempt to downplay the intrusion of privacy relative to the content surveillance program. His statements to Melissa Block on National Public Radio ("NPR") (which were not submitted before the *Hepting* decision) clearly acknowledge the call records program:

> BLOCK: You're saying that you are read into it. I'm curious then if you're saying that you have had oversight directly of ***the program as has been reported, under which the NSA has collected millions of phone records of domestic calls.***
>
> Senator ROBERTS: Well, basically, ***if you want to get into that, we're talking about business records***. We're not, you know, we're not listening to anybody. This isn't a situation where if I call you, you call me, or if I call home or whatever, that that conversation is being listened to.

Ex. P at 2 (All Things Considered, May 17, 2006) (emphasis added). Likewise, CBS News' Gloria Borger reported that Senator Roberts stated that "the NSA was looking at the phone calls collected during the surveillance, but he said not at the content, just at the pattern of phone calls." Ex. Q at 1 (May 16, 2006). His statements alone confirm an NSA program exists to collect call records, distinct from the content surveillance program, under a "business records" rationale.

Senator Roberts is a reliable, fully informed source for the information he disclosed. He has been "read into" (*i.e.*, briefed on) the operational details of the program since its inception, "along with Senator Rockefeller, and along with our two counterparts in the House and along with the leadership." Ex. P at 2.[4] Senator Roberts attended briefings on the programs on ten occasions over a period of more than three years. Ex. S at 2-3 (John D. Negroponte Letter, May 17, 2006). He had even "actually gone out and seen the program at work." Ex. P at 2.

Senator Roberts was not the only member of the Senate Intelligence Committee who was in-the-know and publicly defending the Administration's collection of call records as mere collection of "business records." An interview with Senator Kit Bond on PBS Online (which was also not submitted before the *Hepting* decision) leaves no doubt about the program's existence:

---

[4] Indeed, as the White House noted, "all intelligence matters conducted by the National Security Agency—and we've said this many times—have been fully briefed to a handful of members of the Senate Intelligence and House Intelligence Committees and to the leadership." Ex. R at 1 (White House Press Briefing, May 16, 2006).

JIM LEHRER: … You're a member of the Senate Intelligence Committee. Did you know about this?

SEN. KIT BOND, R-Mo.: Yes. I'm a member of the ***subcommittee*** of the Intelligence Committee ***that's been thoroughly briefed*** on ***this*** program and other programs….

Now, to move on to the points, number one, my colleague, Senator Leahy, is a good lawyer, and I believe that he knows, as any lawyer should know, that ***business records*** are not protected by the Fourth Amendment….

JIM LEHRER: Excuse me, Senator Leahy, and let me just ask just one follow-up question to Senator Bond so we understand what this is about.

What these are, are records. And nobody then—now, these are—but ***there are tens of millions of records that are in this database, right***? And they say somebody, Billy Bob called Sammy Sue or whatever, and that's all it says, and then they go and try to match them with other people?

SEN. KIT BOND: First, let me say that I'm not commenting on in any way any of the allegations made in the news story today. ***I can tell you about the president's program***.

The president's program uses information collected from phone companies. The phone companies keep their records. They have a record. And it shows what telephone number called what other telephone number.

Ex. T at 4-5 (May 11, 2006) (emphasis added). Senator Bond was also briefed numerous times on these issues, as a member of the subcommittee of the Senate Select Committee on Intelligence that had oversight of the NSA programs. *See* Ex. S at 3 (Mar. 9 & 10, 2006 meetings).

Even before the disclosures by Senators Roberts and Bonds, Former Senate Majority Leader William Frist spoke out in defense of the call records programs to CNN's Wolf Blitzer:

BLITZER: Let's talk about the surveillance program here in the United States since 9/11. USA Today reported a bombshell this week. Let me read to you from the article on Thursday.

"The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans using data provided by AT&T, Verizon and BellSouth...."

Are you comfortable with ***this program***?

FRIST: ***Absolutely. Absolutely. I am one of the people who are briefed…***

BLITZER: You've known about this for years.

FRIST: I've known about ***the program***. I am absolutely convinced that you, your family, our families are safer because of ***this particular program***.

Ex. U at 18 (CNN Late Edition, May 14, 2006) (emphasis added).[5]

In response to the uproar over the call records program reported by *USA Today,* the White House announced that NSA Director, General Keith Alexander, would brief the full membership of both the House and Senate Intelligence Committees on the "[f]ull terrorist surveillance program," including "the entire scope of NSA surveillance," not to be "limited to the program that the President has publicly acknowledged." Ex. V at 1-2, 8 (White House Press Briefing, May 17, 2006). Following those briefings, *USA Today* reported that ***nineteen*** "[m]embers of the House and Senate intelligence committees confirm that the National Security Agency has compiled a massive database of domestic phone call records," and that "[t]he program collected records of the numbers dialed and the length of calls." Ex. W at 1 (USA Today, June 30, 2006). Further, several members of Congress spoke on the record. Senator Saxby Chambliss, bemoaning BellSouth's refusal to participate, opined that "[i]t probably would be better to have records of every telephone company." *Id.* at 2. According to Senator Ted Stevens, the records program targeted long-distance, not "cross-city" or "mom-and-pop calls." *Id.* at 2. Senator Orrin Hatch, Rep. Anna Eshoo, and Rep. Rush Holt also made statements on the record acknowledging the program. *Id.* at 3.

Separately, Representative Jane Harman has noted that "there is a program that involves the collection of some phone records." Ex. X at 8 (Congressional Hearing, Mar. 14, 2007). This makes nine members of Congress, each fully briefed on "the entire scope of NSA surveillance," [6] who have acknowledged the call records program publicly and on-the-record.

3. Verizon, as Well as Qwest, Has Confirmed the Call Records Program.

As noted in the *Hepting* decision, Qwest has unequivocally confirmed requests by the Government for "private telephone records of Qwest customers," which Qwest refused after learning that it would not be provided with any lawful authority permitting such access. 439

---

[5] As part of the Senate leadership, Senator Frist was also briefed on the program. *See* Ex. P at 1, Ex. R at 1, Ex. S at 2-3 (Negroponte letter).

[6] Representative Harman is a member of the subcommittee that received numerous briefings on the NSA programs on at least eight occasions. Ex. S at 2-3.

F. Supp. 2d at 988; *see also* Ex. Y at 1 (Wall St. J. Online, May 12, 2006).[7] At that time, no other telecommunications company had acknowledged that it had been asked to provide customer call records. Now, Verizon Wireless also admits it was asked by the Government to hand over private phone records, through a pre-recorded statement by a Regional President, Kelly Kurtzman, reported by PBS's Lee Hochberg on *Newshour*:

> LEE HOCHBERG: Privacy advocate Hendricks . . . notes, after 9/11, the Bush administration asked phone companies for billions of private phone records.
>
> Federal law forbids turning them over without a court order, but most phone companies did so anyway. Verizon's landline division was hit with a $50 billion consumer lawsuit for doing so. ***Verizon Wireless emphasizes it withheld its phone records***.
>
> KELLY KURTZMAN: ***Absolutely, absolutely. We were asked, but we said, no, we would not give that information***, again, you know, trying to protect the privacy of our customers. We take that very seriously.

Ex. Z at 3 (PBS Online NewsHour, April 11, 2007).

As confirmed by Verizon, Qwest, the President, and the informed members of Congress quoted above, the existence of the call records program is now anything but secret.

C. The Facts Regarding Verizon's and MCI's Participation in the Content and Records Programs Is Not a Secret.

Unlike AT&T, which refused to either confirm or deny the existence of a content surveillance or call records program (*see Hepting,* 439 F. Supp. 2d at 989), Verizon has not remained silent. The recent statement by Kelly Kurtzman makes clear that Verizon was asked to turn over call records. Meanwhile, Verizon's other public statements, although couched as denials, tacitly admit that its newly-acquired subsidiary MCI is also implicated in the turnover of records to the government. These admissions corroborate widespread public acknowledgement that "the N.S.A. has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications." Ex. I at 1.[8]

---

[7] According to Joseph Nacchio, "Chairman and CEO of Qwest [who] was serving pursuant to the President's appointment as the Chairman of the National Security Telecommunications Advisory Committee," the refusal to comply was based on a "disinclination on the part of the authorities to use any legal process" in support of the request. *Id.*

[8] Further, Verizon customer service representatives have told customers that Verizon turned over call records of Verizon wireline customers to the NSA. *See, e.g.*, MCC ¶ 184(3) (on May 11,

Verizon issued a press release on May 12, 2006 stating that, because the call records program was highly classified, Verizon could not "confirm or deny whether we have had any relationship to it." Ex. AA at 1 (Verizon Press Release). As to MCI, it stated: "In January 2006, Verizon acquired MCI, ***and we are ensuring*** that Verizon's policies are implemented at that entity and that all its activities fully comply with law." *Id.* (emphasis added).

As popular uproar over the call records program grew, Verizon issued a second statement four days later in a very different tone. That May 16 statement expressly denied that "Verizon" brand businesses had turned over call records, but tacitly admitted MCI's participation. Ex. BB at 1 (Verizon Press Release). Describing the actions of the company ***prior to*** Verizon's January 2006 acquisition of MCI, it explained:

> From the time of the 9/11 attacks ***until just four months ago, Verizon had three major businesses***-its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of ***these businesses***, or any call data from ***those records***. None of ***these companies*** - wireless or wireline - provided customer records or call data.

Id. (emphasis added). Pressed on the point, Peter Thonis, Verizon's Chief Communications Officer, said the May 12, 2006 denial of participation in the call records program was about Verizon, *not* MCI. *See* Ex. CC at 1-2 (USA Today, May 16, 2006). Verizon's earlier promise to ensure that its policies "are implemented" at MCI, with Verizon's calculated exclusion of MCI from its public denial of involvement must fairly be read as an admission of MCI's participation in the call records program.

MCI's participation was also confirmed in the June 30, 2006 *USA Today* story that followed the full briefing of all members of the Intelligence Committees on all aspects of the NSA's surveillance activities. Ex. W at 1-2. Four intelligence committee members verified that "MCI, the long-distance carrier that Verizon acquired in January, did provide call records to the

---

2006, a "customer service representative told [Michael Colonna of New Jersey] that although the records of *other* Verizon customers were disclosed, the records of Verizon wireless customers were not disclosed;" MCC ¶ 184(1) (on May 12, 2006, Verizon customer service representative Ellen "expressly confirmed to [landline customer Norman LeBoon of Pennsylvania:] . . . 'I can tell you Mr. LeBoon that your records have been shared with the government, but that's between you and me'"); MCC ¶ 184(2) (Verizon customer service representative on May 16, 2006 told Verizon subscriber Mark Baker that "Verizon has turned its subscriber records over to the NSA").

FENWICK & WEST LLP ATTORNEYS AT LAW SAN FRANCISCO

government," while "[f]ive members of the intelligence committees said they were told by senior intelligence officials that AT&T participated in the NSA domestic calls program." *Id.* at 1-2. And, like AT&T, MCI plays a critical role in the long distance and international calling infrastructure targeted under the NSA programs. Before the merger, MCI was the second largest long distance carrier with "14 million residential customers and about a million corporate customers. Ex. DD at 1 (N.Y. Times, Feb. 14, 2005).[9] Indeed, a majority of international calls are handled by long-distance carriers AT&T, MCI, and Sprint. Ex. FF at 1 (USA Today, Feb. 6, 2006).

Verizon's ubiquity in providing telecommunications services is also beyond dispute. As of year-end 2006, Verizon's wireline network included more than 45 million access lines nationwide, with approximately 13 million miles of local, inter-city and long-distance fiber-optic systems. Ex. GG. at 4 (Recent Verizon History).

D. Verizon's and MCI's Turnover of Call Records to the Government Is a Public Fact Well Known to Potential Terrorists.

Verizon's May 16, 2006 press release confirms that, like AT&T, Verizon is committed to assisting the government with national security programs, stating that: "Verizon always stands ready, however, to help protect the country from terrorist attack," and "[w]hen asked for help, we will always make sure that any assistance is authorized by law and that our customers' privacy is safeguarded." Ex. BB at 1. Its May 12, 2006 press release similarly emphasized that "Verizon will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes." Ex. AA at 1. As is apparent from its Motion to Dismiss, Verizon, like AT&T, "at least presently believes that any such assistance would be legal if [it] were simply a passive agent of the government." *Hepting*, 439 F. Supp. 2d at 992.

Verizon's cooperation is further confirmed by the government's recent reports on the FBI's call record collections. The FBI's general counsel, Valerie Caproni, testified before Congress that both Verizon and MCI have current contracts with the FBI to provide telephone toll billing records. Ex. HH at 45 (Congressional Hearing, Mar. 20, 2007). She confirmed details revealed by a March 2007 report by the DOJ's Office of Inspector General (Ex. II, "IG's Report," Mar. 2007) about numerous abuses by Verizon, MCI and AT&T in turning over reams of telephone toll records.

---

[9] In 2003, MCI received 20.8 percent of all long distance toll service revenues, trailing only AT&T. Ex. EE at 9-11, 9-12 (FCC Report, June 21, 2005).

The IG's Report harshly criticized the way the FBI has exercised its authority to obtain customer call records through the issuance of National Security Letters ("NSLs") to Verizon, MCI and AT&T.[10] The FBI issued 143,074 separate NSL requests during 2003 to 2005 alone; the "overwhelming majority" of which sought "telephone toll billing records information, subscriber information (telephone or e-mail) or electronic communication transactional records." *Id.* at 36. In just nine of those NSLs, the FBI requested subscriber information on 11,100 separate telephone numbers. *Id.* Their contracts enabled Verizon and MCI to "provide 'near real-time servicing'" of records requests and meet the FBI's need to quickly obtain billing data. *Id.* at 88.

Further, beyond the abuses of NSLs, "one of the [IG's] most troubling findings" was that the "FBI improperly obtained telephone toll billing records and subscriber information from three telephone companies [Verizon, MCI and AT&T] pursuant to over 700 so-called exigent letters." Ex. HH at 10 (Inspector General, Glenn A. Fine testifying). In response to these exigent letters, Verizon and MCI provided call records to the FBI prior to receiving either an NSL or a grand jury subpoena. *See* Ex. II at 89-90. The phone companies not only acted "contrary to the provisions of the contracts," *id.* at 90; the IG also concluded that such use of exigent letters, without first issuing NSLs, violated the NSI Guidelines and internal FBI policies. *Id.* at 92-93. A subsequent internal FBI audit also disclosed thousand of potential violations of law or agency rules while collecting data about domestic phone calls, e-mails and financial transactions in recent years, "far more than was documented" in the IG's report. Ex. JJ at 1 (Wash. Post, June 14, 2007).

---

[10] NSLs are written directives from the FBI to third parties instructing them to provide specific records which include telephone subscriber information or toll billing records. *Id.* at 1-2. To obtain approval to issue an NSL, an FBI agent must determine that the information is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities and, with respect to an investigation involving a 'U.S. person,' is 'not solely conducted on the basis of activities protected by the First Amendment.'" *Id.* at 22. Every NSL must be approved and signed by an appropriate certifying official (either the Special Agent in Charge or specified designees at FBI Headquarters). *Id.* at 24.

The very public IG report, Senate testimony, and Verizon's press releases leave no doubt that Verizon and MCI are turning over customer calling records. Moreover, because NSLs may seek any records the FBI claims are "relevant to an authorized investigation to protect against international terrorism[,]" Ex. II at 13, *see also* 18 U.S.C. § 2709, requests are not limited to records of an identified suspect. Indeed, the IG noted use of NSLs to access information about individuals who are *"two or three steps removed* from their subjects without determining if these contacts reveal suspicious connections." *Id.* at 109 (emphasis added). Thus, potential terrorists who may not believe they are themselves yet suspects know that their records will nonetheless be captured if they communicate even indirectly with suspects.

Terrorists also know that other members of the intelligence community, including the NSA, may access records collected in response to NSLs. *See* 18 U.S.C. § 2709(d) (FBI may disseminate information and records obtained under this section pursuant to Attorney General's guidelines for foreign intelligence collection and counterintelligence investigations); *see also* Ex. KK at 11, 24-29 (Guidelines for FBI National Security Investigations). As the IG reported, records provided in electronic format are uploaded into a massive "Telephone Applications database," which "contains raw data derived from NSLs, known as 'metadata,' including the call duration." Ex. II at 28 & n.59. From 2003 to 2005, approximately 2,000 non-FBI personnel had accounts permitting them to access this specialized application for telephone record data. *Id.* The records were also periodically uploaded into an Investigative Data Warehouse (the "IDW"), a centralized repository of over 560 million FBI and other agency records with "advanced search capabilities." *Id.* at 30 & n.64, 53. Finally, the "raw data" consisting of telephone numbers or account information may be packaged in "Intelligence Information Reports," *id.* at 54, and disseminated to other members of the intelligence community, including the National Security Agency. *Id.* at 59; *id.* at 47 (diagram showing FBI disseminates "Intelligence Information Reports" to NSA).

All of these very public confirmations would lead any terrorist to conclude that by using Verizon or MCI—or communicating with those who did—his calling records would be exposed to regular and ongoing surveillance and/or analysis when requested by the government.

ANALYSIS

I. THIS COURT IN *HEPTING* APPLIED THE PROPER STANDARDS FOR ANALYSIS OF THE STATE SECRETS PRIVILEGE.

The Government's Motion to Dismiss depends on the premise that "the Court's analysis [in *Hepting*] did not reflect a proper application of the standard of review." Gov. Brief at 18. In fact, this Court's application of the legal standards in *Hepting* was correct. The Executive's dispute of those standards provides no basis to reverse this Court's conclusions.

A. The Judiciary, Not the Executive, Determines the Applicability and Effect of the State Secrets Privilege.

The state secrets privilege does not confer upon the Executive branch unilateral authority to terminate unwanted litigation at the pleading stage—whether brought against the Government itself, or, as here, against private parties.

"The state secrets privilege is a common law evidentiary privilege that allows the government to *deny discovery* of military secrets." *Kasza v. Browner*, 133 F.3d 1159, 1165 (9th Cir. 1998) (emphasis added). Thus, unlike the *Totten/Tenet* bar, *see infra* at Section IV, even when the state secrets privilege is properly invoked, it generally does not require dismissal. Instead, "the result is simply that the [secret] evidence is unavailable, as though a witness had died, and the case will proceed accordingly, with no consequences save those resulting from the loss of the evidence." *Ellsberg v. Mitchell*, 709 F.2d 51, 56 (D.C. Cir. 1983); *see also Kasza*, 133 F.3d at 1166 ("the plaintiff's case then goes forward based on evidence not covered by the privilege"). Thus, where the plaintiff has "sufficient admissible evidence to enable a fact finder to decide in its favor without resort to the privileged material, then the potential helpfulness to plaintiff's case of other secret, inadmissible information is not grounds for dismissal. . . . The superiority of more direct, but unavailable proof does not invalidate findings of fact rationally based on the circumstantial evidence which is before the fact finder." *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 271, 274 (4th Cir. 1980), *rev'd en banc on other grounds*, 1980 U.S. App. LEXIS 11406 (4th Cir. 1980). Thus, cases holding that the privilege necessitates dismissal at the pleading stage are exceedingly rare. *See infra*, Section II.A.

Moreover, it is up to *the Court*—not the Government—to decide whether the state secrets privilege applies in a particular case. *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953) ("*the Court itself must determine* whether the circumstances are appropriate for the claim of privilege") (emphasis added). Indeed, while the privilege has been characterized as "absolute" when it applies, the law is clear that the Judiciary retains its traditional and vital role in determining the circumstances in which the Executive's assertion of the privilege should be accepted in the first instance. *See id.* at 9-10 ("judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers"); *see also In re United States*, 872 F.2d 472, 475 (D.C. Cir. 1989) ("[A] court must not merely unthinkingly ratify the executive's assertion of absolute privilege, lest it inappropriately abandon its important judicial role.").[11]

Accordingly, it is only *after the Court is satisfied* that there is a "reasonable danger that national security would be harmed by the disclosure of state secrets" that the privilege will be applied. *Kasza*, 133 F.3d at 1166; *see also, Ellsberg*, 709 F.2d at 57 ("the privilege may not be used to shield any material not strictly necessary to prevent injury to national security; and, whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter"). The Court must determine whether "the showing of the harm that might reasonably be seen to flow from disclosure is adequate in a given case to trigger the absolute right to withhold the information sought in that case." *Halkin v. Helms*, 690 F.2d 977, 990 (D.C. Cir. 1982).

Contrary to the Government's assertion, this Court properly exercised this power of independent review in *Hepting*. In recognizing that "even the state secrets privilege has its limits," this Court "respect[ed] the executive's constitutional duty to protect the nation from threats [while] tak[ing] seriously its constitutional duty to adjudicate the disputes that come before it." *Hepting*, 439 F. Supp. 2d at 995 (citing *Hamdi v. Rumsfeld*, 542 U.S. 507, 536

[11] The Judiciary's exercise of independent review over assertions of the privilege plays a critical role in sustaining governmental checks and balances. "Concentration of power puts personal liberty in peril of arbitrary action by officials, an incursion the Constitution's three-part system is designed to avoid." *Hamdan v. Rumsfeld*, 126 S. Ct. 2749, 2800 (2006) (Kennedy, J., concurring). *See also Public Citizen v. U.S. DOJ*, 491 U.S. 440, 468 (1989) (Kennedy, J., concurring) ("It remains one of the vital functions of this Court to police with care the separation of the governing powers. . . . When structure fails, liberty is always in peril.").

FENWICK & WEST LLP
ATTORNEYS AT LAW
SAN FRANCISCO

(2004)). No less than in *Hepting*, "dismissing this case at the outset would sacrifice liberty for no apparent enhancement in security." 439 F. Supp. 2d at 995.

B. The Court Must First Find the Information to be Secret Before Reasonable Harm from Disclosure Could Become Relevant.

As this Court recognized in *Hepting*, determining whether the state secrets privilege applies in a given case involves two questions. *See Hepting*, 439 F. Supp. 2d at 986, 990. "The first step . . . is determining whether that information actually is a 'secret.'" *Id.* at 986. The second step, assuming the information is secret, is determining whether its verification or substantiation "possesses the potential to endanger national security." *Id.* at 990. *Both* questions must be answered in the affirmative in order for the privilege to apply. *Accord Al-Haramain Islamic Found. v. Bush*, 451 F. Supp. 2d 1215, 1221 (D. Or. 2006) ("Prior to determining whether the state secrets privilege requires dismissal of plaintiff's case, [the court] first determine[d] whether this information qualifies as a secret."); *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 913 (N.D. Ill. 2006) ("The question the Court must determine is whether the information sought by the plaintiffs is truly a secret or whether it has become sufficiently public to defeat the government's privilege claim.").

The Government argues that in *Hepting* this Court "substitute[d] its judgment for the judgment of the most senior members of the intelligence community" and "appeared to avoid assessing the harms of disclosure identified by the DNI through its own analysis of the statements by AT&T and Government and conclusions that it drew from these statements." Gov. Brief at 19. The Government's criticism of *Hepting* fails to grasp the distinction between the two inquiries at issue in the state secrets determination. Although both must be satisfied to establish entitlement to the privilege, the secrecy-in-fact inquiry logically precedes the question of reasonable harm. *See Hepting*, 439 F. Supp. 2d at 986, 990. Certainly, the Executive's claim of the likely harm flowing from disclosure of secret information is entitled to some measure of deference. *Kasza*, 133 F.3d at 1166; *see also In re United States*, 872 F.2d at 475-76. But this claim guides the Court in the second inquiry, not the first. To the extent the putative secret has *already* been revealed through reasonably reliable public statements, claims of harm flowing from confirmation or discovery of a *non-secret* are immaterial. *See Hepting*, 439 F. Supp. 2d at 994.[12]

Thus, even assuming the Executive may "occupy a position superior to that of the courts in evaluating the consequences of a release of sensitive information," *El-Masri v. United States*, 479 F.3d 296, 305 (4th Cir. 2007), the Executive can claim no unique ability to determine which facts have been publicly disclosed. Given its impartiality, the Court is better positioned to guard, as it must, against self-serving claims of privilege by the Executive, particularly where it is the Executive that is asserted to have overstepped its lawful authority. *See Reynolds*, 345 U.S. at 9-10; *see also ACLU v. Brown*, 619 F.2d 1170, 1173 (7th Cir. 1980) (*en banc*) ("*in camera* review of documents allegedly covered by the privilege" is necessary to avoid "permit[ting] the Government to classify documents just to avoid their production even though there is need for their production and no true need for secrecy"). Indeed, the Government's objection to this Court's engaging in "its own analysis" of the facts (Gov. Brief at 19) would reduce the Judiciary to a mere functionary of the Executive. Such an outcome cannot be squared with the Supreme Court's insistence that "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." *Reynolds*, 345 U.S. at 9-10.

1. Information Publicly Disclosed by Reliable Sources Is Not Secret.

The state secrets privilege is not a tool designed to shield from examination awkward facts or unpleasant realities. It exists to preclude discovery of secret information that, in addition, presents a reasonable threat of harm to national security if disclosed. *Kasza*, 133 F.3d at 1166. Where disclosure has already occurred, the government has no power to retract information from the public sphere. *See infra* note 13.

While not every unconfirmed public report renders previously secret information a matter of public knowledge, where the source's relationship to the underlying facts "possesses substantial indicia of reliability," the published information can no longer reasonably be termed

[12] *See also Kasza*, 133 F.3d at 1165 ("[t]he state secrets privilege . . . allows the government to deny discovery of military *secrets*") (emphasis added); *Capital Cities Media, Inc. v. Toole*, 463 U.S. 1303, 1306 (1983) ("restrictions on the publication of information that would have been available to any member of the public" not permitted); *McGhehee v. Casey*, 718 F.2d 1137, 1141 (D.C. Cir. 1983) ("The government has no legitimate interest in censoring unclassified materials" or information "derive[d] from public sources.").

secret. *Hepting*, 439 F. Supp. 2d at 990 (considering reliable "public admissions or denials by the government, AT&T and other telecommunications companies, which are the parties indisputably situated to disclose whether and to what extent the alleged programs exist"). Other courts facing widely disseminated putative "state secrets" likewise have examined the Executive's claims of privilege in light of reliable contrary information.[13]

The Court in *Terkel* followed this Court's lead, accepting as bearing "persuasive indication of reliability" both government reports and "admissions or denials by private entities claimed to have participated in purportedly secret activity." 441 F. Supp. 2d at 913. The court noted that, "[i]n particular, public admissions by the government about the specific activity at issue ought to be sufficient to overcome a later assertion of the state secrets privilege." *Id.*

2. The Government's Claim that It Has Not Intentionally Waived the Privilege Cannot Cloak Non-Secret Information.

The Government is wrong in insisting that, because it has not officially "waived" the state secrets privilege, this Court must ignore the impact of public disclosures regarding the NSA's surveillance programs. This argument is a red herring.

Here, as in *Hepting*, the question is not whether the state secrets privilege has been waived; the question is whether the Government is entitled to claim the privilege in the first place, *i.e.*, whether sufficient reliable information in the public record demonstrates that the information sought to be concealed by the privilege is not a secret. The public disclosures made by the Executive, the Congress, and the telecommunications carriers asked to participate in the NSA's

[13] *See, e.g., Al-Haramain*, 451 F. Supp. 2d at 1222, 1224 (contrary to the Government's argument, "the existence of the Surveillance Program is not a secret, the subjects of the program are not a secret, and the general method of the program—including that it is warrantless—is not a secret"); *Jabara v. Kelley*, 75 F.R.D. 475, 492-493 (E.D. Mich. 1977) (concluding that "it would be a farce to conclude that the name of this other federal agency remains a military or state secret" where "[t]he name of this other federal agency has been revealed in a final report of the United States Senate Select Committee on Intelligence"); *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006) (sufficient information about NSA warrantless surveillance program had been made public to proceed to merits of plaintiff's claim without any risk to national security); *Spock v. United States*, 464 F. Supp. 510, 520 (S.D.N.Y. 1978) ("Here, where the only discussion in issue is the admission or denial of the allegation that interception of communications occurred[,] an allegation which has already received widespread publicity[,] the abrogation of the plaintiff's right of access to the courts would undermine our country's historic commitment to the rule of law.").

surveillance programs, *see supra* at pp. 5-11, are directly relevant to this inquiry. In arguing that the privilege has not been "waived," the Government has put the cart before the horse.

Public disclosure of information is very different from the concept of waiver, a legal term of art. Waiver refers to "an intentional relinquishment or abandonment of a known right or privilege." *Barker v. Wingo*, 407 U.S. 514, 525 (1972) (quoting *Johnson v. Zerbst*, 304 U.S. 458, 464 (1938)). It presupposes an applicable right or privilege in the first instance, regardless of who holds the authority to waive. *Pengate Handling Sys. v. Westchester Surplus Lines Ins. Co.*, No. 1:06-CV-0993, 2007 U.S. Dist. LEXIS 13303, at *10 n.5 (M.D. Pa. Feb. 27, 2007) ("Waiver is irrelevant if the privilege does not apply.").[14] The Government cannot shift focus away from its inability to *establish* secrecy by insisting it has not *waived* it.

Although the Government may prefer that only intentional statements by authorized members of the Executive can render secret information non-secret, that is not the way of the world. This Court's analysis in *Hepting* was correct, and its application in this case likewise cannot justify dismissal on the pleadings.

3. Truly Secret Information Is Subject to the Privilege Only if Disclosure Threatens National Security.

Even where information actually remains secret, the Court must also determine whether its disclosure poses a reasonable threat of harm. *Hepting*, 439 F. Supp. 2d at 990. Only if the Court finds "a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged" is discovery precluded on that particular evidence. *Reynolds*, 345 U.S. at 10. Thus, the Court must still "be satisfied that under the particular circumstances of the case" a reasonable danger to national security exists. *Kasza*, 133 F.3d at 1166; *see also In re United States*, 872 F.2d at 475-76. On the other hand, the Court

[14] *See also* 26 Wright & Graham, *Fed. Prac. & Proc.* § 5665 ("[T]he secrecy required for the privilege can be destroyed without regard to who made or authorized the disclosure."); *Scanlon v. Bricklayers & Allied Craftworkers, Local No. 3*, No. 05-CV-628A(F), 2007 U.S. Dist. LEXIS 29798, *17-18 (W.D.N.Y. Apr. 23, 2007) ([W]here defendants failed to establish that the attorney-client privilege was applicable, it was "not necessary to consider defendants' argument that there was no waiver of the privilege"); *Sedco Int'l, S. A. v. Cory*, 683 F.2d 1201, 1205 (8th Cir. 1982)("No contention can be made that the attorney-client privilege precludes disclosure of factual information.") (citing *Upjohn Co. v. United States*, 449 U.S. 383, 395-96 (1981)).

must reject the privilege if it finds disclosure presents no reasonable threat of harm. *See Reynolds*, 345 U.S. at 10; *see, e.g.*, *Al-Haramain*, 451 F. Supp. 2d at 1224 (under the circumstances, "no harm to the national security would occur").

To make this determination in *Hepting*, this Court assessed "the value of the information to an individual or group bent on threatening the security of the country." *Hepting*, 439 F. Supp. 2d at 990. It recognized that whether individuals inclined to commit acts threatening the national security engage in rational calculations remains "an open question." *Id.* But this Court adopted what may be termed a "reasonably prudent terrorist" standard, under which the likelihood of any potential harm to national security is gauged against the utility of disclosure to a hypothetical rational opponent. *Id.* This test, and its broader analytical framework, were proper in *Hepting*, and remain appropriate here. *See also Terkel*, 441 F. Supp. 2d at 913 (adopting this Court's analysis, but applying it to call records program in the absence of many of the public admissions now presented here).

II. "THE VERY SUBJECT MATTER" OF THIS LITIGATION IS NOT A SECRET; ACCORDINGLY THE GOVERNMENT'S ASSERTION OF THE STATE SECRETS PRIVILEGE CANNOT BAR ALL CLAIMS AT THE OUTSET.

Even after this Court's order to show cause why the *Hepting* ruling does not govern these cases, the Government makes no effort to distinguish the facts relating to Verizon and MCI from those applicable to AT&T. The Government thinks that the facts make no difference. But, of course they do. And, as this Court noted, additional facts or confirmation of earlier allegations often emerge during the course of litigation. *Hepting*, 439 F. Supp. 2d at 1001. As this Court predicted, disclosures have only continued since *Hepting* was decided, and they now plainly include public acknowledgment of the turnover of call records as well as intercepted content. As shown below, both the existence of and Verizon's and MCI's relationships to these programs are anything but secret. Accordingly, the "very subject matter" of these actions cannot be deemed a state secret. Unless this Court's analytical framework in *Hepting* was mistaken—which it was not—the state secrets privilege cannot bar claims against Verizon and MCI.

A. Dismissal is a Draconian Remedy Unsupported by Precedent Here.

The Government argues that these cases should be dismissed before any discovery has occurred because the very subject matter of the actions is a state secret. As the Court recognized in *Hepting*, it is a rare case indeed that is dismissed at the outset on this basis. *Hepting*, 439 F. Supp. 2d at 993 ("[N]o case dismissed because its 'very subject matter' was a state secret involved ongoing, widespread violations of individual constitutional rights, as plaintiffs allege here. Indeed, most cases in which the 'very subject matter' was a state secret involved classified details about either a highly technical invention or a covert espionage relationship."). Indeed, courts have recognized that "[d]ismissal of a suit, and the consequent denial of a forum without giving the plaintiff her day in court . . . is indeed draconian." *In re United States*, 872 F.2d at 477; *see also Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1242 (4th Cir. 1985) ("[D]enial of the [Judicial] forum provided under the Constitution is a drastic remedy that has rarely been invoked.").

In truth, not *one* of the cases cited by the Government actually supports its position. Gov. Brief at 16, 21. To begin with, both *Kasza* and *Fitzgerald* involved dismissals that occurred well *after* the pleading stage. In *Kasza*, dismissal occurred subsequent to both discovery and summary judgment motions, when it became obvious that the "plaintiff [could not] prove the *prima facie* elements of her claim with nonprivileged evidence." 133 F.3d at 1166. In *Fitzgerald*, the Fourth Circuit upheld dismissal of the plaintiff's libel claim on the basis that there was no way plaintiff could demonstrate the falsity of the allegedly libelous statements without revealing military secrets, but only after years of litigation and pretrial preparation. 776 F.2d at 1238 n.3.[15]

The few cases offered by the Government that actually involved dismissal on state secrets grounds at the pleading stage are readily distinguishable. In *El-Masri*, the plaintiff claimed that he had been illegally detained and interrogated by the CIA. 479 F.3d at 299. The Fourth Circuit concluded that, to establish his claims, El-Masri would have been required to prove the "details of

[15] The Government also relies on *Clift v. United States*, 808 F. Supp. 101 (D. Conn. 1991), a case that was litigated for well over a decade. *See* Gov. Brief at 21 n.10. Clift filed suit in 1976; after he sought discovery of allegedly secret information the district court dismissed his claims on state secrets grounds. 808 F. Supp. at 102. Although the Second Circuit agreed that discovery of the secret information was unavailable, it vacated the dismissal, holding that plaintiff had a right to pursue his claims using non-privileged evidence. *Clift v. United States*, 597 F.2d 826, 830 (2d Cir. 1979). Only twelve years later, after Clift demonstrated his "inability to marshal additional nonprivileged evidence," were his claims dismissed. 808 F. Supp. at 104. *Clift* hardly supports dismissal at the pleading stage as the Government demands here.

CIA espionage contracts" and "the roles, if any, that the defendants played in the events he alleges." *Id.* at 309. The Court dismissed on the theory that "evidence that exposes how the CIA organizes, staffs, and supervises its most sensitive intelligence operations" was "so central to the subject matter of the litigation that any attempt to proceed w[ould] threaten disclosure of the privileged matters." *Id.* at 306, 309; *see also Hepting*, 439 F. Supp. 2d at 994 (distinguishing *El-Masri* on this same ground). Similarly, in *Zuckerbraun v. Gen. Dynamics Corp.*, the court affirmed dismissal of a negligence claim alleging negligent design and manufacture of a Navy weapons system. 935 F.2d 544, 546 (2d Cir. 1991). Because the design of the weapons—the central factual dispute of the plaintiff's claim—was itself a state secret and plaintiff lacked "any sources of reliable evidence" of negligent design, dismissal was appropriate. *Id.* at 548. The two remaining cases relied upon by the Government required discovery into the employment histories and personnel decisions of the nation's intelligence agencies themselves.[16]

Here, in stark contrast, the subject matter of this case focuses not on details of the intelligence apparatus, but "only on whether [the carriers] intercepted and disclosed communications or communications records to the government." *Hepting*, 439 F. Supp. 2d at 994. As this Court observed, Plaintiffs' claims do not necessarily require inquiry into methods by which the Government obtains access to their communication or records, or what the Government does with information once obtained. Rather, it is the mere fact of disclosure by *Defendants*—in the absence of compliance with the relevant statutory procedures—that is

[16] In *Sterling v. Tenet*, the Fourth Circuit dismissed a CIA agent's claims of employment discrimination because they would have required him to present secret evidence about "the relative job performance of [CIA] agents, details of how such performance is measured, and the organizational structure of CIA intelligence-gathering." 416 F.3d 338, 347, 341 (4th Cir. 2005), *cert. denied*, 126 S. Ct. 1052 (2006). Likewise, in *Edmonds v. United States*, the court dismissed the plaintiff's claims where she would be required to prove "the nature of plaintiff's employment[,] . . . the events surrounding her termination[,] . . . the content of what may be contained in a system of records and who had access to it." 323 F. Supp. 2d 65, 79-81 (D.D.C. 2004), *aff'd*, 161 Fed. Appx. 6 (D.C. Cir. 2005). "[B]ecause the Court [found] that documents related to the plaintiff's employment, termination and security review that comprise the system of records are privileged," the case could not proceed. *Id.* at 81.

The Government also cites *Maxwell v. First Nat'l Bank*, 143 F.R.D. 590 (D. Md. 1991), *aff'd*, 998 F.2d 1009 (4th Cir. 1993). Gov. Brief 16 n.8. Although *Maxwell* made reference to other cases dismissing claims on the basis of the state secrets privilege, 143 F.R.D. at 598-99, that case did not involve a motion by the Government to dismiss the plaintiff's claims, much less at the outset of the case. *Id.* at 600.

sufficient to establish Plaintiffs' claims. *See In re NSA Telcoms. Records Litig.*, 483 F. Supp. 2d 934, 944-45 (N.D. Cal. 2007) ("*Riordan* Remand Order") ("the exact procedures allegedly used to disclose the records are of little consequence to plaintiffs' legal theories. . . . [T]he particular methods defendants used to submit the customer calling records to the NSA would not matter; absent a statutory exemption, mere disclosure is enough.").

In short, the Government has failed to cite a single factually analogous case supporting its insistence that this case be dismissed at the pleading stage. As discussed below, the public record suffers from no shortage of disclosures revealing the central subject of Plaintiffs' claims.

B. The Public Record Reveals the Existence of the Programs and the Participation of MCI and Verizon.

1. The Existence of the Content Monitoring Program Is Not Secret.

As this Court rightly concluded in *Hepting*, because of "public disclosures by the government and AT&T," the existence of a widespread program of intercepting and monitoring domestic communications is "hardly a secret." *Hepting*, 439 F. Supp. 2d at 994. There, this Court concluded that the government has publicly "admitted the existence" of the program, that it "monitor[s] communication content," "tracks calls into the United States or out of the United States," and "operates without warrants." *Id.* at 992 (internal quotations and citations omitted). Other courts have agreed.[17]

The Government contends that "disproving Plaintiffs' allegation of a content surveillance dragnet would require demonstrating what the United States *is* doing," thereby "revealing specific intelligence sources and methods about the TSP that the DNI and NSA Director have explained must be protected." Gov. Brief at 11. But as this Court recognized in *Hepting*, the President and Attorney General have already described in detail the alleged scope of the TSP program; protests that the TSP's contours "must remain secret" cannot depublicize that information. *Id.*; *Hepting*, 439 F. Supp. 2d at 996. Indeed, "the government has disclosed the universe of possibilities in

[17] *See Al-Haramain*, 451 F. Supp. 2d at 1222 ("the existence of the Surveillance Program is not a secret, the subjects of the program are not a secret, and the general method of the program—including that it is warrantless—is not a secret"); *ACLU v. NSA*, 438 F. Supp. 2d at 765 (Plaintiffs established "*prima facie* case based solely on Defendants' public admissions regarding the TSP").

terms of whose communications it monitors and where those communicating parties are located." *Id*. "[T]he exact procedures" and "particular methods" employed by the program are of no consequence, and, to the extent they are secret, need not be disclosed.

Moreover, this Court also found it significant that the Government has denied the existence of the broader content program, a denial that the Government repeats in its brief here. Gov. Brief at 51. As the Court rightly concluded, those denials "opened the door for judicial inquiry." 439 F. Supp. 2d at 996. "[I]f the government has not been truthful, the state secrets privilege should not serve as a shield for its false public statements." *Id.* Regardless of the secret status of the particular operational details of the program, which are, in any event, far from the "very subject matter" of this litigation, the existence of the Government's warrantless content surveillance program is not subject to the state secrets privilege.

2. The Existence of the Call Records Program Is Not Subject to the State Secrets Privilege.

Although a year ago the Court was "hesitant to conclude that the existence or non-existence of the communications record program necessarily constitutes a state secret," *Hepting*, 439 F. Supp. 3d at 997, no tenable claim of secrecy remains. The confirmation of that program is now undeniable and comes in the form of on-the-record statements by fully informed and reliable witnesses from the Executive branch, the Congress, and Verizon itself.

a. Executive Disclosures Reveal the Existence of the Call Records Program.

Both President Bush and Attorney General Gonzales have acknowledged the existence of a program "that has been fully briefed to members of the United States Congress" and entails "the NSA compiling a list of [Americans'] telephone calls." *See supra* at p. 5; *see also* Ex. N at 2-3; Ex. O at 6-7 (Gonzales defending program). While not revealing the details of the operation of the program, these on-the-record comments confirm that the very subject of this litigation—the existence of a call records program—is not a secret. *Cf. Hepting*, 439 F. Supp. 2d at 996 (relying on statements of the President and Attorney General).

b. Congressional Disclosures Reveal the Existence of the Call Records Program.

More illuminating than the rather cryptic admissions of the Executive are statements of members of Congress who have been fully briefed on the call records program. Nine members of Congress who have been briefed on and/or observed the program have provided *on-the-record* confirmation of its existence; *USA Today* reported confirmation by nineteen members. Five confirmed AT&T's participation and four confirmed MCI's. *See supra* at pp. 5-8. Against these consistent acknowledgements, not a single member of Congress or the Executive branch has denied—or even cast doubt upon—the program's existence. Any "reasonably prudent terrorist" engaging in the sort of risk versus efficiency calculations postulated by the Court (*see Hepting*, 439 F. Supp. 2d at 990) must assume that the program exists and that AT&T and MCI were, and may still be, its largest participants.

Both the Government and Verizon chose to ignore these Congressional disclosures in their opening papers, although they were highlighted in Class Plaintiffs' Consolidated Response to Order to Show Cause (Dkt. No. 155). Yet, even if the Executive *prefers* to disseminate information through its own channels, the reliability of governmental disclosures, whether gauged by this Court or our nation's enemies, is not confined to statements by the Executive. Courts have acknowledged that Legislative statements can eliminate secrecy, and in cases involving disclosures far less than these. In *Jabara*, the plaintiff sought disclosure of the name of a federal agency that had admittedly intercepted his communications. 75 F.R.D. at 490. Where the name of this agency previously had been revealed in a report of the United States Senate Select Committee on Intelligence, the privilege was unavailable since, according to the court, "it would be a farce to conclude that the name of this other federal agency remains a military or state secret." *Id.* at 492-93;[18] *see also Ellsberg*, 709 F.2d at 61 n.47 (reversing dismissal of the

[18] *Terkel* took issue with *Jabara* to the extent it was cited for the notion that "once executive officials have disclosed certain activities to members of Congress, those activities are no longer covered by the state secrets privilege." *Terkel*, 441 F. Supp. 2d at 914. Plaintiffs make no such argument here; rather, they argue merely that if legislators intimately involved with the program make authoritative, on the record, public disclosures defending it on national broadcasts, no claim of secrecy can survive. Nor does *Halkin* challenge the proposition that congressional statements are sufficiently reliable to undermine claims of secrecy. There the court simply held that the

FENWICK & WEST LLP ATTORNEYS AT LAW SAN FRANCISCO

plaintiff's claims where congressional disclosure "detract[ed] from the government's ability to rely on inferences drawn from the 'surrounding circumstances' in justifying its privilege claim").

Salisbury v. United States, 690 F.2d 966 (D.C. Cir. 1982), offers no reason to disregard the statements of fully-briefed Members of Congress. *See* Verizon Motion to Dismiss the MCC at 4. As the court explained, in rejecting Plaintiff's Freedom of Information Act ("FOIA") request, "bare discussions by this court and the Congress of NSA's methods generally cannot be equated with disclosure by the agency itself of its methods of information gathering." *Id.* at 971. This statement, offered in connection with Plaintiff's FOIA request rather than the government's state secret claim, merely reiterates the uncontroversial proposition that the disclosure of general facts about a program does not necessarily compel further disclosure of its operational details. *Salisbury* in no way intimates that, where Senators and Representatives acknowledge the existence of an intelligence program in an effort to publicly defend it, the Executive remains free to assert, in response to a legal challenge, that the very existence of that same program is a secret. Our notions of judicial review have not yet stepped that far through the looking glass.

These congressional disclosures should be accorded equal weight to the statements of the Executive and telecommunications providers recognized as reliable in *Hepting*. In light of these statements, the Government cannot maintain that the program's existence remains secret.

c. Party Disclosures Reveal the Existence of the Call Records Program.

The record of disclosures by telecommunications companies also presents far stronger confirmation of the records program than was present in *Hepting*. In a lawsuit against Verizon, public admissions through a current Verizon Regional President that Verizon was asked to turn over billions of private phone records, Ex. Z at 3, carry even more "indicia of reliability" than the earlier public statements offered by the former CEO of Qwest. *See Hepting*, 439 F. Supp. 2d at 988, 990 ("telecommunications providers" are "indisputably situated to disclose whether and to

---

disclosure of some general information through "congressional committees investigating intelligence matters" did not eliminate the threat posed by further disclosure of detailed information *not* previously revealed through that investigation. *Halkin v. Helms*, 598 F.2d 1, 10 (D.C. Cir. 1978).

what extent the alleged programs exist").[19] "[A]dmissions or denials by private entities . . . may, under appropriate circumstances, constitute evidence supporting a contention that the state secrets privilege cannot be claimed as to that particular activity. Like official governmental disclosures, such statements reasonably may be considered reliable because they come directly from persons in a position to know whether or not the supposedly covert activity is taking place." *Terkel*, 441 F. Supp. 2d at 913. Taken together, the statements of Verizon and Qwest, the revelations from members of Congress, and the disclosures from the Executive leave no *reasonable* doubt as to the existence of the call records program.[20]

3. Participation by MCI and Verizon in Both the Content and Records Programs Is Not Secret.

In addition to establishing the existence of the content monitoring and call records programs, reliable publicly disclosed information renders the participation or non-participation in those programs by MCI and Verizon non-secret.

a. The Participation of Verizon and MCI in the Content Surveillance Program Is Not Secret.

Attorney General Gonzales has already disclosed the general contours and existence of the NSA program involving "intercepts of contents of communications," Ex. B at 1, whereby "the N.S.A. has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications." Ex. I at 1. As in

---

[19] The preliminary ruling in *United States v. Adams*, 473 F. Supp. 2d 108 (D. Me. 2006) supports no different result. That court, in an attempt to "preserve the status quo," granted the government a temporary restraining order and preliminary injunction precluding, pending review by this Court, enforcement of the Maine PUC's order that Verizon confirm the content of its press releases. *Id*. at 121. The *Adams* court asked the parties to "understand the temporal constraints under which the district court labored in arriving at its decision," which afforded "precious little time with the press of other matters to research and write a decision on an issue of manifest public significance, due within hours of oral argument." *Id*. at 114 n.7. In giving any consideration to *Adams*, we respectfully suggest this Court bear the same in mind.

[20] The Government's argument that the Court may not rely "on statements made by a private party in attempting to decide whether information is properly protected under the privilege," Gov. Brief at 19, n.9, makes the same mistake as its argument that only the Government can "waive" the state secrets privilege, discussed *supra* at Part I(B)(2). "The secrecy required for the privilege can be destroyed without regard to who made or authorized the disclosure." 26 *Wright & Graham*, Fed. Prac. & Proc. § 5665.

Hepting, "[c]onsidering the ubiquity of [MCI & Verizon's] telecommunications services, it is unclear whether this [communications content] program could even exist without [MCI & Verizon's] acquiescence and cooperation." *Hepting*, 439 F. Supp. 2d at 992. *See supra* at p. 10- (detailing Verizon's 14 million residential customers, 45 million wirelines, millions of miles of fibre optic cable). Moreover, much like AT&T, Verizon has stated that it "always stands ready" to assist the government when it believes, as it claims to here, that the law allows its cooperation. Ex. BB at 1. Thus, like AT&T, Verizon's "assistance in national security surveillance is hardly the kind of 'secret' that the *Totten* bar and the state secrets privilege were intended to protect or that a potential terrorist would fail to anticipate." *Hepting*, 439 F. Supp. 2d at 993.

b. Participation by Verizon's MCI Subsidiary in the Call Records Program Is Not Secret.

Verizon has affirmatively taken over responsibility for MCI's activities with respect to the call records program, publicly stating that it is now "ensuring that Verizon's policies are implemented at [MCI] and that all its activities fully comply with the law." Ex. AA at 1. Meanwhile, even as it denied its own participation in the program, Verizon first carved out MCI from that denial, then explicitly disavowed any denial as to MCI. *Compare* Ex. AA (May 12, 2006 press release) with Ex. BB (May 16, 2006 press release); *see also* Ex. CC at 1-2. The implications of Verizon's carefully crafted public statements are unmistakable, providing far greater certainty of MCI's participation than ever pertained to AT&T.

Congressional disclosures likewise have laid bare MCI's participation in the records program. *See supra* at pp. 5-8; Ex. W at 2. Such participation is hardly surprising since, like AT&T, MCI plays a critical role in the long distance and international calling infrastructure targeted under the NSA programs. Most international calls are handled by long-distance carriers AT&T, MCI, and Sprint, Ex. FF at 1, again rendering "it [ ] unclear whether this program could even exist without [MCI's] acquiescence and cooperation." *Hepting*, 439 F. Supp. 2d at 992. These public disclosures make it impossible to pretend that MCI's participation remains a secret. They also make it impossible to dismiss this case at the outset against either MCI itself or Verizon, which has now acquired and assumed responsibility for MCI.

c. **Verizon's Direct Participation in the Call Records Program Is Not Secret.**

Although Verizon initially refused to "confirm or deny whether we have any relationship to [the call records program]," Ex. AA at 1, Verizon subsequently parted with AT&T by issuing a highly publicized statement expressly denying that "Verizon" brand phone and internet businesses turned over call records. *See Hepting*, 439 F. Supp. 2d at 988-89; *supra* at p. 10. Verizon's very publicly proclaimed non-participation renders its status no longer a secret and fairly subject to confirmation under oath.

Verizon made the choice whether or not to speak. Having attempted to negate its role, Verizon cannot use the state secrets privilege to protect against judicial inquiry. *Id.* at 996 ("the state secrets privilege should not serve as a shield for its false public statements"). Just as "the government opened the door for judicial inquiry by publicly confirming and denying material information about its monitoring of communication content," *id.*, so have Verizon's statements opened the door—with or without the government's approval. Having publicized its denial, Verizon can now assert its non-participation as a *defense*. But no one can assert it is a secret.[21]

d. **Testing Verizon's Participation Through More Formal Means Will Not Harm National Security.**

In *Hepting*, after the Court concluded AT&T's assistance in surveillance was not sufficiently secret to halt the litigation, the Court determined that "revealing whether AT&T has received a certification to assist in monitoring communication content should not reveal any new information that would assist a terrorist and adversely affect national security." 439 F. Supp. 2d at 996. By analogy, the Court should conclude here that confirming Verizon's roles will not reveal new information that would materially assist a terrorist or impact national security.

---

[21] The *Riordan* Plaintiffs intend to amend their complaint to add (1) an express allegation that Verizon Communications, Inc. has controlled and bears responsibility for the actions of MCI following the acquisition, and (2) claims directly against MCI's California operating entities, because MCI is Plaintiff Dennis Riordan's long distance service provider. *Riordan* Compl. ¶ 9. Thus, if this Court concluded that only MCI's participation in the call records program is not secret, the *Riordan* Plaintiffs' claims could proceed. The *Riordan* Plaintiffs sought a stipulation allowing them to amend now without impacting the briefing or hearing schedule, but Verizon refused.

FENWICK & WEST LLP ATTORNEYS AT LAW SAN FRANCISCO

In fact, the public record already reveals that Verizon and MCI routinely provide massive volumes of call records to federal intelligence agencies, pursuant to contracts designed to provide "real time" access to customer calling records. The General Counsel of the FBI and the DOJ Inspector General have admitted that Verizon and MCI voluntarily provided such records on thousands of occasions when no legal authorization was first obtained under the NSL process. *See supra* at pp. 11-13. Much like AT&T in *Hepting*, there is no doubt that "[Verizon] helps the government in classified matters when asked, and [Verizon] at least currently believes, on the facts as alleged in plaintiff's complaint, its assistance is legal." 439 F. Supp. 2d at 993.

Thus, additional confirmation of the turnover of records without judicial process will not assist a rational terrorist, who already has ample reason to expect Verizon will turn over his calling records to federal authorities, with or without legal process. From the terrorist's point of view, given the other intelligence agencies' ability to access call record information obtained by the FBI, *supra* at pp. 11-13, it makes little difference which intelligence agency initially collects this information. Confirmation of Verizon's participation in the NSA's call records program, therefore, will not alter the communications methods employed by the "reasonable" terrorist.

Finally, the Government's very public announcement of Verizon's and MCI's contracts to provide call records to the federal intelligence agencies demonstrates that the Government is asserting the "secrecy" of the carriers' conduct only when convenient. The turnover of call records is the very subject of this litigation. The Government's willingness to disclose such events demonstrates that this very subject cannot always be a secret. The *Terkel* Court, in distinguishing *Tenet* and *Weinberger*, put it well:

> "***Disclosing the mere fact that a telecommunications provider is providing its customer records to the government, however, is not a state secret without some explanation about why disclosures regarding such a relationship would harm national security***. Put another way, the Court cannot think of a situation in which publicly acknowledging a covert espionage contract or a secret nuclear weapons facility would not threaten national security. In contrast, the ***Court can hypothesize numerous situations in which confirming or denying the disclosure of telephone records to the government would not threaten national security and would clearly reveal wholesale violations of the plaintiffs' statutory rights***."

Terkel, 441 F. Supp. 2d at 907-08 (emphasis added). Here, the government has already demonstrated its own belief that disclosure of the mass turnover of call records will not necessarily threaten national security. And Plaintiffs have demonstrated good reason to suspect a wholesale violation of their statutory and constitutional rights. The very subject of this litigation therefore is not a state secret, and the Court should, as in *Hepting*, adjudicate Plaintiffs' claims by assessing state secrets not *ab initio*, but as the individual evidentiary issues arise.

III. THESE CASES MAY NOT BE DISMISSED AT THE PLEADING STAGE BASED ON THE HYPOTHESIS THAT PLAINTIFFS MAY BE UNABLE TO ESTABLISH A *PRIMA FACIE* CASE, THAT DEFENSES MAY BE UNAVAILABLE, OR THAT PLAINTIFFS MAY BE UNABLE TO PROVE STANDING.

A. Mere Speculation That Evidence Needed to Establish a *Prima Facie* Case or Defense May Be Unavailable Cannot Support Dismissal.

Where, as here, the very subject matter of litigation is not a state secret, dismissal can occur on state secrets grounds only if the Court is satisfied "after further proceedings, [that] the plaintiff cannot prove the *prima facie* elements of her claim," *Kasza*, 133 F.3d at 1166, or that "the privilege deprives the defendant of information that would otherwise give the defendant a valid defense." *Id.* at 1166 (quoting *Bareford v. Gen. Dynamics Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992)); *see also Ellsberg*, 709 F.2d at 65 (remanding case to determine if plaintiffs can prove *prima facie* case without privileged information); *Clift*, 597 F.2d at 830 (same).

Because such dismissal would necessarily depend on the significance of potentially unavailable items of evidence, Plaintiffs must be afforded "at least some discovery" and a context to assess the significance of the missing evidence before dismissal is appropriate. *See Hepting*, 439 F. Supp. 2d at 994; *Kasza*, 133 F.3d at 1166. Nonetheless, the Government and Verizon insists on dismissal, not because any identified item of evidence has been excluded due to privilege, but rather on the basis of its hypothesis that evidence that *might* be critical to the case *might* prove undiscoverable. Such surmise cannot preclude discovery.

Aside from being premature, the Government's contention that Plaintiffs are unable to establish their *prima facie* case is mistaken. *See* Gov. Brief at 31. This Court has recognized that Plaintiffs' case turns on the question of interception or disclosure by Verizon and MCI; it does not require Plaintiffs to establish the details of the Government's acquisition or use of the information. *See Riordan* Remand Order, 483 F. Supp. 2d at 944-45 ("the exact procedures allegedly used to disclose the records are of little consequence . . . [and] the particular methods defendants used to submit the customer calling records to the NSA would not matter; . . . mere disclosure is enough."); *Hepting*, 439 F. Supp. 2d at 994. As noted above, neither the existence of the challenged programs nor Defendants' participation remains a secret. *See supra* at pp. 5-11. The state secrets privilege, therefore, imposes no barrier to Plaintiffs' ability to establish a *prima facie* case.

Likewise, given the posture of this litigation, the argument that Verizon will be prevented from proving necessary defenses is entirely premature. Defendants have yet to serve an Answer asserting any defenses. Nor has this Court had the opportunity to rule as to the applicability of the privilege to any particular evidence sought to establish such a defense, or an evidentiary record permitting the Court to assess the availability of a defense on the basis of non-privileged evidence. The mere possibility that Verizon or MCI may choose to raise a defense, that may require one item of evidence instead of another, that may in turn be subject to the state secrets privilege, is far too attenuated a chain to justify dismissal at the outset of a case of this import.

In *Hepting*, this Court faced nearly identical arguments and rightly concluded that discovery on potential defenses was necessary before consideration of dismissal was appropriate. *Hepting*, 439 F. Supp. 2d at 996-97. As to AT&T's potential certification defense, the Court understood that, because the existence of the content program was not a secret, "the state secrets privilege will not prevent AT&T from asserting a certification-based defense." *Id.* Accordingly, it recognized that AT&T could "confirm or deny the existence of a certification . . . through a combination of responses to interrogatories and *in camera* review by the court." *Id.* at 997. The same is true for Verizon and MCI. Likewise, the state secrets privilege need not prevent Defendants' presentation of a defense, however tenuous, based on federal statutes. *See* Verizon MTD at 20-22. Only after real evidence is adduced or withheld can that determination occur.

Once this Court determines the very subject matter of this litigation is not a secret, discovery should proceed. *Hepting*, 439 F. Supp. 2d at 994. Further efforts to dispose of this litigation will turn on the outcome of a careful discovery process, not the parties' speculation.

B. The Government's Hypothesized Lack of Standing Provides No Basis for Dismissal on the Pleadings.

The Government also tries to subvert the discovery process by insisting that the state secrets privilege prevents Plaintiffs from establishing standing. This attempt also fails.

Neither the Government nor Verizon seriously contends these complaints should be dismissed on the ground that Plaintiffs have failed to adequately *plead* standing.[22] Nor could they. The allegations of the complaints are more than sufficient. *See, e.g.,* MCC ¶¶ 169-71, 173-74, 203, 212, 226, 233, 238, 245. Rather, the Government argues here, as it did in *Hepting*, that it is entitled to summary judgment because Plaintiffs cannot *prove*—before discovery—that the communications or records of any individual Plaintiff were intercepted and/or disclosed. *See Hepting*, Dkt. No.124 at pp. 16-20 (Government's argument for summary judgment that Plaintiffs had burden to "prove standing"). The Government's current motion should be denied for the following reasons, each of which we discuss in detail below.

First, the Government's motion is premature. The Government takes the position that its very assertion of the state secrets privilege deprives Plaintiffs of the ability to establish standing. That is not the case. Before the Court may evaluate the Government's argument that Plaintiffs cannot *presently* prove standing, there must first be a ruling on the Government's assertion that the very subject matter of this litigation is a state secret. That ruling will determine whether the case proceeds to discovery, in which event discovery of particular evidentiary facts will directly bear on the standing issue. Indeed, given the ever-changing state of available information concerning these programs, it is particularly premature to determine standing before Plaintiffs have had any opportunity to develop a factual record. The Government's prove-standing-now arguments ignore traditional principles for assessing standing at each appropriate stage of the litigation. Plaintiffs are, at a minimum, entitled to discovery pursuant to Fed. R. Civ. P. Rule 56(f) ("Rule 56(f)") before the issue of standing can be addressed on a motion for summary

[22] Although it has filed only a motion to dismiss, Verizon nevertheless briefly argues that the complaint should be dismissed because Plaintiffs will be unable to *prove* standing. Verizon Motion to Dismiss the MCC at 6. Because only the government may assert the state secrets privilege, *Reynolds*, 345 U.S. at 7, the only relevant issue on Verizon's motion to dismiss is whether plaintiffs have *adequately alleged* standing.

judgment.

Second, as in *Hepting*, Plaintiffs here allege the existence of dragnet programs through which Verizon and MCI engaged in the wholesale interception and/or disclosure of their customers' communications and communications records. Thus, as this Court held in *Hepting*, 439 F. Supp. 2d at 1000-01, proof of the programs' existence and participation in them by Plaintiffs' carriers will, by definition, establish the interception and/or disclosure of Plaintiffs' communications and records. Likewise, the dragnet nature of the challenged programs gives rise to a high probability that Plaintiffs' communications and call records have been intercepted and disclosed. This, too, is sufficient to establish standing, which, like all the elements of Plaintiffs' claims, need be proven only by a preponderance of the evidence.

1. The Government's Motion For Summary Judgment is Premature.

a. It Is Not Appropriate to Address Standing Before a Ruling on the Government's Assertion that the Very Subject Matter of this Litigation is a State Secret.

The Government has made its alternative motion for summary judgment on standing to address the possibility that this Court may decline to dismiss the litigation based on either the *Totten/Tenet* argument or the Government's claim that the very subject matter of the litigation is a state secret. Gov. Brief at 39 n.20. However, if the Court rules, as it did in *Hepting*, that the very subject matter of this litigation is *not* a state secret, that will fundamentally alter the landscape of this litigation, including the potential scope of eventual discovery.

In *Hepting*, this Court confronted the same contention that the Government makes here: that the state secrets privilege bars Plaintiffs from establishing standing. In rejecting that claim, the Court noted that, "the state secrets privilege will not prevent plaintiffs from receiving at least some evidence tending to establish the factual predicate for the injury-in-fact underlying their claims directed at AT&T's alleged involvement in the monitoring of communication content." *Hepting*, 439 F. Supp. 2d at 1001 (referring to ruling that plaintiffs would be entitled to discovery on existence of certification). Similarly, the Court reiterated that additional facts might come to light that would alleviate many of the secrecy concerns about the communication records program. *Id.* The Court went on to note that, should that happen, it might very well be possible for Plaintiffs to obtain information about AT&T's "participation, if any," in that program, as well, without running afoul of the state secrets privilege. *Id.*

As detailed above, that observation was prescient. The existence of the records program has been amply confirmed, thus opening the door to further discovery on standing. In short, because the Government's arguments on standing are premised on the assumption that there can be no discovery because the very subject matter of this litigation is a secret, should the Court deny the motion on that ground, the standing argument falls as well.

b. Plaintiffs Are Not Required to *Prove* Standing Before Discovery.

Elements of standing, like all other elements of a plaintiff's case, need only be "supported . . . with the manner and degree of evidence required at the successive stages of the litigation." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). The rule does not change just because the Government has couched its motion to dismiss in the alternative as a summary judgment motion. The Government's claim that Plaintiffs must *prove* standing now, at this initial, pre-discovery stage, goes too far. The Court thus has discretion to treat the motion for summary judgment as a motion to dismiss. *See, e.g., Nat'l Coal. for Students with Disabilities Educ. and Legal Defense Fund v. Scales*, 150 F. Supp. 2d 845, 848 (D. Md. 2001). That is what this Court did in *Hepting*, 439 F. Supp. 2d at 1001, and it should follow that same course here.

Moreover, Plaintiffs have filed herewith a declaration under Rule 56(f) specifying the discovery they should be permitted to conduct before having to respond to a motion for summary judgment—including facts relating to standing. That declaration seeks the same sort of information that this Court held would be available to plaintiffs in *Hepting*, such as evidence testing the truthfulness of the Government's and Verizon's statements as to the existence of the contents program, and the participation in the records program by Verizon and MCI. *See e.g., Hepting*, 439 F. Supp. 2d at 996 ("the government has opened the door for judicial inquiry by publicly confirming and denying material information about its monitoring of communications content").[23] This includes determining whether Verizon and/or MCI have obtained a certification with respect to their participation in either. *Id*. at 996-97. It also includes information, not remotely subject to a claim of state secrets privilege, such as Verizon's and MCI's network architecture and the manner in which they keep their call records, which may tend to confirm which individuals' information is being divulged. Finally, it sets out the means by which Plaintiffs would pursue discovery on other information, already made public.

---

[23] Both the Government and Verizon have opened this door. *See, e.g.,* Ex. HH at 10, 45, (AT&T,

If the Government wishes to claim that particular portions of the evidence sought in discovery are protected by the state secrets privilege, it may do so at the appropriate time, based on a concrete record. If Verizon wishes to assert that the evidence ultimately gathered cannot support standing, that time will come as well. But especially in a case raising such fundamental issues of individual liberty, there is no basis to foreclose all development of the record, once this Court concludes that the very subject of this litigation is not a state secret.

c. Neither *Halkin* Nor *Ellsberg* "Foreclose Litigation" Before Discovery.

Invoking the two *Halkin* cases and *Ellsberg*, the Government insists that "litigation over Plaintiffs' standing is foreclosed" now by the state secrets privilege. Gov. Brief at 45; *see generally* Gov. Brief at 40-46. As this Court has already recognized, those cases do not entitle the Government to summary judgment or dismissal here.

First, none of those cases was dismissed on standing grounds at inception. The dismissal in *Halkin II* came six years after that case was filed, and only after "the parties [had] fought the bulk of their dispute on the battlefield of discovery" regarding the propriety of *specific* discovery requests. *Halkin II*, 690 F.2d at 984. In *Ellsberg*, dismissal occurred only after more than four years of detailed discovery that occurred in two phases, in which the Government ultimately admitted intercepting the conversations of five of the 16 plaintiffs. 709 F.2d at 53, 54, 55. In *Hepting*, this Court followed this same path and allowed discovery. 439 F. Supp. 2d at 994.

Moreover, neither the *Halkin* cases nor *Ellsberg* support the proposition that plaintiffs in a *dragnet* surveillance and disclosure case must prove that a specific communication by a specific

---

Verizon and MCI have contracts to provide Government with "toll billing information"); Ex. Z at 3, (Kurztman statement that Verizon was asked by Government to provide customer phone records).

plaintiff has been intercepted. Rather, those cases involved *targeted* surveillance programs, as to which this Court has already recognized a fundamental difference from the cases now pending. *Hepting*, 439 F. Supp. 2d at 1000.

The *Halkin* cases are particularly instructive on this point. *Halkin I*'s analysis of the state secrets privilege focused on an NSA surveillance operation that selected messages to individuals on a targeted "watchlist" compiled from a larger group of messages seized by monitoring targeted international communications circuits. *Halkin I*, 598 F.2d at 4, 11 & n.8; *see also*, *Halkin II*, 690 F.2d at 983 & n.23. *Halkin I* applied the privilege because "confirmation or denial of acquisition of *a particular individual's* international communications" could provide valuable information about the reasoning behind the surveillance and about the methods used in carrying it out. 598 F.2d at 8. The same is not true here, both because Plaintiffs allege programs of untargeted dragnet surveillance and in light of public disclosures that Verizon and MCI have contracts to provide call records in near-real time—for example, in connection with foreign intelligence gathering through the use (or misuse) of NSLs. *See supra* at p. 12.

In *Halkin II*, *after further discovery* and pretrial proceedings, the plaintiffs were unable to obtain proof that any of *their* calls had been intercepted, because the appearance of their names on the watchlist did not mean that their calls were being monitored. Rather, if a message *mentioned* a name on the watchlist, the message would be monitored, regardless of whether the named person was actually a party to the conversation. *Halkin I*, 598 F.2d at 11 & n.8; *Halkin II*, 690 F.2d at 983 & n.23. Unlike the "watchlist" of *Halkin II*, in this case of dragnet surveillance, as long as the named plaintiffs were Verizon and MCI "customers during the relevant time period [as alleged at MCC ¶¶ 24-117], the alleged dragnet would have imparted a concrete injury on each of them." *Hepting*, 439 F. Supp. 2d at 1000.

2. Proof of the Existence of the Content and Records Programs Establishes Standing.

Although not required to do so at this early stage of the proceedings, Plaintiffs have already provided the Court with sufficient evidence potentially to establish a genuine issue of fact as to their ability to establish standing. *See* Fed. R. Civ. P. 56; *Central Delta Water Agency v.*

FENWICK & WEST LLP ATTORNEYS AT LAW SAN FRANCISCO

United States, 306 F.3d 938, 947 (9th Cir. 2002) (at summary judgment). As in *Hepting*, if the Court believes that Plaintiffs can provide, or obtain through discovery or other means, some evidence of standing, the Government's motion should be denied. *See Hepting*, 439 F. Supp. 2d at 1001.

a. Establishing that the Dragnet Programs Exist Establishes Plaintiffs' Standing.

The core grievance alleged by Plaintiffs is the operation of a dragnet that sweeps in all communications and records. As this Court recognized in *Hepting*, these allegations are sufficient to establish standing. The same analysis applies here:

> [T]he gravamen of plaintiffs' complaint is that [Verizon and MCI have] created a dragnet that collects the content and records of its customers' communications. . . . The court cannot see how any one plaintiff will have failed to demonstrate injury-in-fact if that plaintiff effectively demonstrates that all class members have so suffered. . . . As long as the named plaintiffs were, as they allege, [Verizon/MCI] customers during the relevant time period . . . , the alleged dragnet would have imparted a concrete injury on each of them."

Hepting, 439 F. Supp. 2d at 1000 (distinguishing *Halkin II*, 690 F.2d at 999-1001); *see also id.* at 1001 ("this dragnet necessarily inflicts a concrete injury that affects each customer in a distinct way, depending on the content of that customer's communications and the time that customer spends using [the carrier's] services").[24]

Just as these allegations are sufficient to establish standing at the pleading stage, *proof* of these allegations at a subsequent stage, after appropriate discovery, will establish standing sufficient to defeat summary judgment. Indeed, substantial information is already available. *See supra* at pp. 5-13. Moreover, the Government is simply wrong when it asserts that its denial of the existence of the dragnet content program obligates Plaintiffs to come forward, before any discovery, with evidence rebutting that denial. To the contrary, as this Court has already held, by issuing a denial, "the government has opened the door for judicial inquiry" *Hepting*, 439 F. Supp. 2d at 996, including on the question of the existence of a certification. *Id.* at 996-97.

Similarly, the existence of the call records program has now been confirmed by on-the-

[24] *See* MCC ¶¶ 163-178 (alleging a dragnet that collects and discloses their customers' communications and records); MCC ¶¶ 24-117 (alleging that each of the named plaintiffs was a Verizon or MCI customer during the relevant time period).

FENWICK & WEST LLP ATTORNEYS AT LAW SAN FRANCISCO

record statements of members of Congress who have been briefed on and observed the program, as well as by Verizon and Qwest. *See supra* pp. 5-8. Plaintiffs are also entitled to discovery on Verizon's participation in the call records program, since it is no secret that Verizon provides call records to the Government for terrorism investigations. *See supra* pp. 11-13. Since the mere existence of a dragnet records program will be sufficient to create standing here, Plaintiffs are entitled to prove such a program, and will have no need for allegedly secret information as to such operational details as what the government does with the information collected.

In sum, here, as in *Hepting*, the Court should "not conclude at this juncture that plaintiffs' claims would necessarily lack the factual support required to withstand a future jurisdictional challenge based on lack of standing." 439 F. Supp. 2d at 1001.

b. Plaintiffs Can Establish Standing to Sue for Damages for Past Injuries and to Enjoin Probable Future Injuries.

The dragnet nature of the programs challenged here is significant for purposes of standing for another reason as well: even in the absence of certainty at this stage of the proceedings, given the likelihood that Plaintiffs' calls and records have been and will be caught up in the dragnets, Plaintiffs have standing to proceed. These programs are, by design, intended to sweep up all communications and all call records. MCC ¶¶ 169-71, 173-74, 203, 212, 226, 233, 238. Moreover, the programs have been in place for years. *See, e.g.,* Exs. H at 1, I at 1 (reporting that TSP or "warrantless surveillance" began after September 11, 2001). It is therefore inconceivable that of the thousands of communications made and received by Plaintiffs during this period, not one of Plaintiffs' calls or call records was swept up in these programs. While the Government argues that this is not sufficient, the certainty of injury it demands is simply not required.

As to the future, "the courts of appeals have generally recognized that threatened harm in the form of an increased risk of future injury may serve as injury-in-fact for Article III standing purposes." *Baur v. Veneman*, 352 F.3d 625, 633 (2d Cir. 2003) (plaintiff had standing to challenge USDA regulations that increased likelihood that beef carrying "mad cow disease" could be sold, based on an allegation that plaintiff ate meat regularly).[25] As to the past, the courts have

[25] *See also, Helling v. McKinney*, 509 U.S. 25, 35 (1993) (allowing Eighth Amendment claim

also consistently allowed plaintiffs to sue based upon past events, even where they cannot prove with certainty that they personally suffered the injury.[26] As the Ninth Circuit has observed "a credible threat of harm is sufficient to constitute actual injury for standing purposes." *Central Delta Water Agency*, 306 F.3d at 949. Certain harms are "'by nature probabilistic,' yet an unreasonable exposure to risk may itself cause cognizable injury." *Baur*, 352 F.3d at 634 (quoting *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 160 (4th Cir. 2000)).[27]

Here, Plaintiffs' allegations easily establish likelihood-of-injury to support standing on the pleadings. As Plaintiffs allege that they were regular users and subscribers of Verizon and MCI since 2001, MCC ¶¶ 24-117, and that Verizon and MCI have used, are using and will continue to use their dragnet to intercept and disclose Plaintiffs' communications and communications, MCC ¶¶ 169-71, 173-74, 203, 212, 226, 233, 238, there is a high likelihood that at least one call or call record of each Plaintiff was intercepted in the past *and* will be intercepted in the future. *See, e.g.,* MCC ¶ 212 ("[t]here is a strong likelihood that Defendants are now engaging in and will continue to engage in the above-described divulgence of Plaintiffs' and Class members'

---

based on allegations that prison officials had "exposed him to levels of [second-hand smoke] that pose an unreasonable risk of serious damage to his future health"); *American Library Ass'n v. FCC*, 401 F.3d 489, 493 (D.C. Cir. 2005) (where librarians' association sought review of an FCC rule, injury-in-fact could be established by showing "that there is a substantial probability that the FCC's order will harm the concrete and particularized interests of at least one of their members"); *Hall v. Norton*, 266 F.3d 969, 976 (9th Cir. 2001) (plaintiff had standing to challenge government's exchange of land with private developer under Clean Air Act based on allegation that new development could aggravate his respiratory discomfort).

[26] *See, e.g., Clinton v. New York*, 524 U.S. 417, 432 (1998) (New York had standing to challenge line item veto law where President vetoed provision that New York could have used as a "statutory 'bargaining chip,'" based on reasoning that "the cancellation inflicted a sufficient likelihood of economic injury to establish standing under our precedents"); *Covington v. Jefferson County*, 358 F.3d 626, 641 (9th Cir. 2004) (holding that evidence of leakage of ozone-depleting materials was "sufficient to show injury in fact because the failure to comply with [the Clean Air Act] has increased the risk of harm to the Covingtons' property"); *Baur*, 352 F.3d at 641 ("as we have clarified, the relevant 'injury' for standing purposes may be exposure to a sufficiently serious risk of medical harm—not the anticipated medical harm itself").

[27] *See also Int'l Bhd. of Teamsters v. TSA*, 429 F.3d 1130, 1134 (D.C. Cir. 2005) (to establish standing on summary judgment, the plaintiff need only "show a 'substantial probability' that it has been injured, that the defendant caused its injury, and that the court could redress that injury") (quoting *Am. Petroleum Inst. v. EPA*, 216 F.3d 50, 63 (D.C. Cir. 2000)); *Walters v. Edgar*, 163 F.3d 430, 434 (7th Cir. 1998) (Posner, C.J.) ("[a] probabilistic harm, if nontrivial, can support standing").

communications"). At minimum, the Court should find Plaintiffs' allegations suffice to establish standing on the pleadings for prospective relief.

3. Plaintiffs Can Establish Standing Via *In Camera* Proceedings.

The purpose of the Article III "case or controversy" requirement is "to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends . . . ." *Baker v. Carr*, 369 U.S. 186, 204 (1962). It is not, as the Government would have it, a cloak of invisibility to be thrown over the courthouse door. Accordingly, to the extent any further demonstration of any Plaintiff's standing was required, it could be provided *in camera*.

If *any* plaintiff has standing, the justiciability requirement is satisfied. *See Dept. of Commerce v. U.S. House of Reps.*, 525 U.S. 316, 330 (1999) (presence of one plaintiff with standing assures that controversy before court is justiciable); *Village of Arlington Heights v. Metro. Housing Dev. Corp.*, 429 U.S. 252, 264 & n.9 (1977) (same). If a single class representative has standing, "there remains no further separate class standing requirement in the constitutional sense." 1A. Conte & H. Newberg, *Newberg on Class Actions* § 2.5, p. 75 (4th ed. 2002) (summarizing cases). Thus, to establish standing, the Court need only satisfy itself—at the appropriate time—that at least *one* of the named Plaintiffs had his or her communications intercepted, and that at least one had his or her call records turned over to the Government.

Further, as recognized in *Hepting*, the courts are to adopt flexible procedures to decide cases involving state secrets. 439 F. Supp. 2d at 1011.[28] If such procedures may be used to adjudicate the case on the merits, *a fortiori*, they can be used to determine whether at least one of the Plaintiffs has been subjected to surveillance of her communications contents and/or records.

Contrary to the Government's argument, confirming that at least one of the Plaintiffs has standing need not reveal anything of consequence which is not already a matter of public record. The Master Complaint names 99 Plaintiffs. *See* MCC ¶¶ 8, 24-117. They reside in 26 states and the District of Columbia. *Id.* They are from large metropolitan areas, and small towns. *Id.*

---

[28] *See Halpern v. United States*, 258 F.2d 36, 43 (2d Cir. 1958) (encouraging "flexible procedure" of *in camera* trial); *Loral Corp. v. McDonnell Douglas Corp.*, 558 F.2d 1130 (2d Cir. 1977) (jury demand properly stricken to preserve confidentiality of classified material); *Spock*, 464 F. Supp. at 520 (endorsing "procedures to safeguard state secrets during this litigation"); *see also infra* at Part VI, discussion of 50 U.S.C. § 1806(f) procedures.

Obviously, Verizon already knows (or can determine) which of these Plaintiffs had their communications intercepted and/or their call records turned over (likely all of them). At the appropriate time, Verizon can be ordered to identify those Plaintiffs to the Court *ex parte* and *in camera*. The Court need only satisfy *itself* that the threshold requirement of standing is satisfied; to the extent there is any secrecy concern, it need not identify *which* Plaintiffs satisfy it, or how many.

As set forth above, the existence of the challenged programs, MCI's participation in the call records program, and Verizon's denial of its own participation are matters of public record. Confirming that one or more of 99 geographically dispersed and demographically diverse Plaintiffs were swept up in these programs would provide a would-be terrorist with no useful information.[29] Accordingly, dismissing the case on such a non-substantive ground "would sacrifice liberty for no apparent enhancement of security." *Hepting*, 439 F. Supp. 2d at 995.

IV. THE *TOTTEN/TENET* BAR DOES NOT APPLY.

In *Hepting*, this Court rejected the government's contention that the action was barred by the Supreme Court's decisions in *Totten v. United States*, 92 U.S. 105 (1875) and *Tenet v. Doe*, 544 U.S. 1, 3 (2005). It held, first, that *Totten* is based on principles of equitable estoppel: one who agrees to spy for the government gives up the right to sue to enforce that agreement because it embodies an implicit promise not to reveal its existence. *Hepting,* 439 F. Supp. 2d at 991. The *Totten* principle does not apply to third parties, such as the plaintiffs in *Hepting*—or to the Plaintiffs here. *Id.* Second, the Court held that the *Totten*/*Tenet* bar does not apply where "[the carrier] and the government have for all practical purposes already disclosed that [the carrier] assists the government in monitoring communication content." *Id.* at 991-92. As discussed above, Verizon and MCI's relationship to the content and records programs have already been disclosed. Both of the Court's rulings in *Hepting* were correct, and both apply with equal force here.

---

[29] Indeed, if necessary to render a finding of standing even more inscrutable, Plaintiffs can amend the complaint to add a number of additional class representatives identified only as "Does," and provide only their names and telephone numbers to the Court and Verizon *in camera*. *See, e.g., Does I through XXIII v. Advanced Textile Corp*., 214 F.3d 1058, 1068, 1070 (9th Cir. 2000) ("a party may preserve his or her anonymity in judicial proceedings . . . when the party's need for anonymity outweighs prejudice to the opposing party and the public's interest in knowing the party's identity;" "Article III's standing requirement does not prevent a court from allowing plaintiffs to proceed anonymously.").

A. *Totten/Tenet* Only Bars Spies from Suing the Government to Enforce Their Espionage Contracts.

In *Hepting*, this Court concluded that *Totten* is based on a rule of estoppel that applies only in the context of suits against the government by its spies. *Hepting*, 439 F. Supp at 991. That conclusion is fully supported by the Supreme Court's decision in *Totten*.

Totten was an action against the government by the administrator of the estate of a former Civil War spy, seeking to enforce his secret espionage contract. The Court held the suit could not be maintained, because the contract contained an implicit promise never to reveal its existence:

> Both employer and agent must have understood that the lips of the other were to be for ever sealed respecting the relation of either to the matter. This *condition of the engagement was implied* from the nature of the employment, and is implied in all secret employments of the government in time of war. . . . The secrecy which such contracts impose precludes any action for their enforcement.

Totten, 92 U.S. at 106-07 (emphasis added).

This Court's interpretation of *Totten* is reinforced by the Supreme Court's recent decision in *Tenet v. Doe*, 544 U.S. 1, which repeatedly characterizes *Totten* in terms of the estoppel that prevents suits against the government by its former spies: "*Totten's* core concern . . . [is] preventing the existence of the *plaintiff's* relationship with the Government from being revealed," *id*. at 10 (emphasis added); "*Totten's* . . . holding [is] that lawsuits premised on alleged espionage agreements are altogether forbidden," *id.* at 9; "the longstanding rule, announced more than a century ago in *Totten*, prohibiting suits against the Government based on covert espionage agreements," *id*. at 3; "the very essence of the alleged contract [in *Totten*] . . . was that it was secret, and had to remain so: [¶] . . . [¶] Thus, we thought it entirely incompatible with the nature of such a contract that a former spy could bring suit to enforce it," *id.* at 7-8; "[n]o matter the clothing in which alleged *spies* dress their claims, *Totten* precludes judicial review in cases such as respondents' *where success depends upon the existence of their secret espionage relationship with the Government*." *Id.* at 8 (emphasis added). In sum, Chief Justice Rehnquist left no doubt in *Tenet* that "only" in a case "filed by an alleged former spy" is "*Totten's* core concern

FENWICK & WEST LLP ATTORNEYS AT LAW SAN FRANCISCO

implicated: preventing the existence of the plaintiff's relationship with the Government from being revealed." *Id.* at 10.[30]

This Court's interpretation of *Totten* is supported by two cases decided since *Hepting*. *See ACLU v. NSA*, 438 F. Supp. 2d at 763; *Terkel*, 441 F. Supp. 2d at 907-08. Finding "that it would be particularly inappropriate to apply *Totten* to this case," *Terkel* explained:

> The plaintiffs in *Totten* and *Tenet* had entered contracts that they knew were a secret, but they nonetheless attempted to bring lawsuits to obtain the benefit of their bargain. In contrast, the plaintiffs in this case were not parties to the alleged contract nor did they agree to its terms; rather, they claim that the performance of an alleged contract entered into by others would violate their statutory rights.

Terkel, 441 F. Supp. 2d at 907. Likewise, the court in *ACLU v. NSA* held:

> This [*Totten/Tenet*] rule should not be applied to the instant case, however, since the rule applies to actions where there is a secret espionage relationship between the Plaintiff and the Government. It is undisputed that Plaintiffs' do not claim to be parties to a secret espionage relationship with Defendants. Accordingly, the court finds the *Totten/Tenet* rule is not applicable to the instant case.

438 F. Supp. 2d at 763 (internal citations omitted).

The Supreme Court's decision in *Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454 U.S. 139 (1981), is not to the contrary. *Weinberger* was decided on the basis of an exemption under FOIA, *not* the *Totten/Tenet* bar. The Court held that because FOIA governs the public disclosure requirements of the National Environmental Policy Act ("NEPA"), and because FOIA Exemption 1 bars disclosure of classified materials, the Navy was excused from disclosures relating to a classified nuclear weapons facility. *Id.* at 145.

Weinberger mentions *Totten* only once, in the decision's penultimate paragraph, simply as another example of a case in which national security concerns defeated the plaintiff's claims:

> ***In other circumstances***, we have held that 'public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated.'

---

[30] The Government misquotes *Tenet* in arguing that the Supreme Court in *Tenet* held *Totten* "was not so limited" as to bar only claims by spies. Gov. Brief at 29. To the contrary, *Tenet*'s "not so limited" statement referred to its rejection of the Court of Appeal's holding that the bar reached only *breach of contract* causes of action, in favor of a rule that the bar also reached any cause of action for due process, equitable estoppel, or other theories in which "alleged spies dress their claims." 544 U.S. at 8. What matters for purposes of the *Totten/Tenet* rule is whether the claim arises out of "the plaintiffs' relationship with the government." *Id.* at 10.

Id. at 146-47 (quoting *Totten*, 92 U.S. at 107) (emphasis added).[31]

Finally, the Fourth Circuit's decision in *El-Masri*, 479 F.3d 296, is a decision applying the state secrets privilege, not the *Totten/Tenet* bar. In contrast to the state secrets privilege, *El-Masri* explained that "*Totten* has come to primarily represent a somewhat narrower principle—a categorical bar on actions to enforce secret contracts for espionage." *Id.* at 306; *see also id.* at 309 (referring to the *Totten/Tenet* bar as "establishing [an] absolute bar to enforcement of confidential agreement to conduct espionage"). Because the *Totten* bar and state secrets privilege share a purpose to protect against disclosure of secret national security information, it is not surprising that *Totten* is often cited in state secrets cases as indicative of the significance and judicial recognition of that objective. But as this Court rightly recognized in *Hepting*, that similar purpose does not conflate these two distinct doctrines.[32]

Like the plaintiffs in *Hepting*, the Plaintiffs in these cases "made no agreement with the government and are not bound by any implied covenant of secrecy." *Hepting*, 439 F. Supp. 2d at 991. Accordingly, the *Totten/Tenet* bar has no application here.

B. Verizon's Public and Admitted Assistance to Government Surveillance Is Not a "Secret" that the *Totten/Tenet* Bar Protects.

As noted in *Hepting*, and as the Supreme Court in *Tenet* confirmed, the *Totten* bar has no application where the existence of an intelligence relationship is publicly known and admitted by the Government. *Hepting*, 438 F. Supp. 2d at 991-92. The court in *Tenet* was quite explicit:

> [T]here is an obvious difference, for purposes of *Totten*, between a suit brought by an acknowledged (though covert) employee of the CIA and one filed by an alleged

---

[31] Not surprisingly, the *Tenet* Court also does not describe *Weinberger* as applying the *Totten* bar; it simply alludes to *Weinberger's* citation of *Totten* as evidence of *Totten*'s continuing validity. 544 U.S. at 9.

[32] The Government argues for an unwarranted extension of *Totten* under which a contractor's public disclosure cannot be considered in determining whether or not his contract remains a state secret when challenged by a third party. Gov. Brief at 19 n.9 and 30-31. This argument errs by conflating the two doctrines. The rule of *Totten* is merely that a spy cannot sue based on a secret relationship, it does not require a court to ignore a contractor's reliable public disclosures in an action to enforce a third party's privacy rights. The argument is also senseless from a policy perspective: while allowing a spy to sue "would invite attempts to undermine the privilege by mere assertions of knowledge by an interested party," (*Hepting*, 439 F. Supp. 2d at 990), the *opposite* is true in this case, as confirmated by Verizon and MCI of their participation in the programs could expose them to *liability*.

FENWICK & WEST LLP ATTORNEYS AT LAW SAN FRANCISCO

> former spy. Only in the latter scenario is *Totten's* core concern implicated: preventing the existence of the plaintiff's relationship with the Government from being revealed.

544 U.S. at 10.[33] Here, as set forth in detail above, the Government and Verizon have already disclosed that Verizon/MCI helps the Government in surveillance of communications content and records. *See supra* pp. 11-13.

This Court has already concluded that public admissions by the Government and telecommunications providers confirm the existence of a widespread NSA program to intercept and monitor American's communications without warrants. *See Hepting*, 439 F. Supp. 2d 987-89, 992; *see also supra* pp. 2-4. In turn, MCI plays a critical roll in the long distance and international calling infrastructure targeted under the NSA programs. *See* Ex. FF at 1.

Further, as set out in detail in the Statement of Facts, on-the-record statements by the Executive Branch, members of Congress who are fully briefed on it, and representatives of Verizon and Qwest, have all confirmed the existence of the records program. *See supra* pp. 5-9. Verizon has tacitly admitted MCI's participation in the records program, *see* Ex. BB at 1, and takes responsibility for participation by the MCI entities in that program. More generally, the FBI's General Counsel, Valerie Caproni, has publicly stated that the federal government has entered into contracts for Verizon and MCI to provide access to customer toll billing information "very quickly." Ex. HH at 45. In light of these and other facts described above, Verizon's and MCI's "assistance in national security surveillance is hardly the kind of 'secret' that the *Totten* bar and the state secrets privilege were intended to protect." *Hepting*, 439 F. Supp. 2d at 993.

V. STATUTORY PRIVILEGES DO NOT BAR DISCOVERY INTO VERIZON'S AND MCI'S ACTIONS, AND IN ANY EVENT, DISMISSAL AT THIS STAGE WOULD NOT BE WARRANTED.

Courts, including this one in *Hepting*, have unanimously held that the two statutory privileges asserted by the NSA do not warrant dismissal in cases exactly analogous to this one. Likewise, dismissal of Plaintiffs' claims against Verizon and MCI is not warranted, because

---

[33] *See also*, *Tenet*, 544 U.S. at 10 n.5 (explaining that "the fact that the plaintiff in *Webster* kept his *identity* secret did not mean that the employment *relationship* between him and the CIA was not known and admitted by the CIA," hence the *Totten* bar did not apply as that relationship had already been revealed) (emphasis in original).

“[n]either of these [statutory privileges] by their terms requires the court to dismiss this action and it would be premature for the court to do so at this time.” *Hepting*, 439 F. Supp. 2d at 998.

As a threshold matter, the two statutory privileges asserted by the Government do not bar Plaintiffs’ claims, which seek discovery from Verizon and MCI, not the federal government. Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1), does not apply because Plaintiffs do not seek disclosure of information from the NSA, DNI, or any other governmental agency—they seek discovery only from Verizon and MCI. *See Terkel*, 441 F. Supp. 2d at 906 (holding on analogous facts involving AT&T that “*section 102A(i)(1)* does not by itself bar prosecution in this case”). Indeed, the statute is relevant “only in that it instructs the Director of National Intelligence to take measures that are available to prevent disclosure regarding intelligence sources and methods—for example, by asserting the state secrets privilege.” *Id.* That has been done.[34]

For similar reasons, dismissal is also not warranted under Section 6 of the National Security Agency Act of 1959. 50 U.S.C. § 402. Section 6 relates generally to the authority of the NSA to withhold certain information from public disclosure. It is trumped here by the more specifically drawn Foreign Intelligence Surveillance Act (“FISA”) statute, codified at 50 U.S.C. sections 1806(f), 1845(f), and 2511(2)(a)(ii)(B). These detailed provisions apply by their terms to electronic surveillance, the subject of this case, whereas Section 6 relates only generally, allowing the NSA to prevent disclosure of information about the “organization or [] function of the National Security Agency.” 50 U.S.C. § 402 note. Accordingly, these later and more specific Congressional enactments prevail over Section 6. *See Edmond v. United States*, 520 U.S. 651, 657 (1997) (specific statutory provision governs when in conflict with general one); *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000) (“[A] specific policy embodied in a later federal statute should control our construction of the [earlier] statute, even though it has not been expressly amended.”) This is particularly true where, as here, “the scope of the earlier

[34] Moreover, disclosure of the information Plaintiffs seek (to the extent not already disclosed) is authorized by Congress under the more specific provisions of FISA at 50 U.S.C. sections 1806(f), 1845(f). By contrast, section 102A(i)(1) operates to prevent only *unauthorized disclosures* of information. 50 U.S.C. § 403-1(i)(1).

statute is broad but the subsequent statutes more specifically address the topic at hand.") (quotation and citation omitted).

Even if the two statutory privileges asserted here could block discovery of certain information from Verizon and MCI, dismissal of Plaintiffs' action is unwarranted at this juncture. Each court that has considered motions to dismiss similar claims brought by plaintiffs challenging the surveillance programs, including this Court, has held that the statutory privileges do not mandate dismissal at the outset of the case, before any discovery. Rather, the courts have properly endorsed a step-by-step application of the privilege as to *particular evidence* as the case progresses. *See Hepting*, 439 F. Supp. 2d at 998 (noting that "[n]either of these provisions by their terms requires the court to dismiss this action").[35]

The cases cited by the Government are distinguishable in that they applied the statutory privileges to requests for documents or information *directly from the NSA or other federal agencies* under FOIA. These cases held only that information sought from the NSA or CIA was shielded from disclosure under exemptions to FOIA based on section 6 and/or 102A(i)(1).[36] They cannot be extended from the limited FOIA context to support the Government's broader proposition that Sections 6 and 102A(i)(1) prohibit all disclosure of "intelligence-related information" generally in civil electronic surveillance cases. Again, such disclosure and discovery is instead governed by the FISA statutes.

---

[35] *See also Al-Haramain*, 451 F. Supp. 2d at 1227 ("[t]he statutory privileges at issue here do not direct the dismissal of this action"; endorsing application of the privileges to specific evidence); *Terkel*, 441 F. Supp. 2d at 905-06 (noting skepticism that section 6 could "allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA" and denying dismissal under section 102A(i)(1)).

[36] *See e.g., People for the Am. Way Found. v. NSA Cent. Sec. Serv.*, 462 F. Supp. 2d 21 (D.D.C. 2006) (documents withheld by NSA were shielded from FOIA disclosure under Section 6 as a statutory exemption); *CIA v. Sims*, 471 U.S. 159, 177 (1985) (Director of CIA authorized to withhold information under FOIA exemptions); *Fitzgibbon v. CIA*, 911 F.2d 755 (D.C. Cir. 1990) (same for FOIA requests to CIA and FBI). *Terkel*, 441 F. Supp. 2d at 905, distinguished the Government's other section 6 cases on the same ground. The remaining case cited by the Government, *Snepp v. United States*, 444 U.S. 507 (1980), does not relate to the statutory privileges asserted here.

FENWICK & WEST LLP
ATTORNEYS AT LAW
SAN FRANCISCO

VI. EVEN IF THE SUBJECT MATTER WERE SECRET, THE EXECUTIVE CANNOT IGNORE EXPLICIT PROCEDURES CONGRESS ESTABLISHED FOR REVIEW OF THE REQUESTED INFORMATION.

Even if the Government somehow could establish its claim to the state secrets privilege, Congress has foreclosed any threshold dismissal on state secrets grounds by establishing specific procedures for judicial review and, if necessary, appropriate limited disclosure of secret information relating to electronic surveillance. Congress, in the proper exercise of its authority, has declared that FISA is the exclusive means for conducting electronic surveillance and that § 1806(f) provides the exclusive procedure by which claims of state secrets are to be examined and adjudicated in the context of foreign intelligence surveillance. The Executive is not free to disregard this clear congressional mandate.

A. Congress May Properly Limit Executive Authority by Statute.

The Executive may not ignore a statute lawfully created by Congress. *See, e.g.*, *United States v. Nixon*, 418 U.S. 683, 715 (1974) (the President is not "above the law"). This principle is rooted in the "doctrine of the separation of powers [] adopted by the Convention of 1787." *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S, 579, 629 (1952) (Douglas, J., concurring) (quoting *Myers v. United States*, 272 U.S. 52, 293 (1926) (Brandeis, J., dissenting)). This "central judgment of the Framers of the Constitution … is essential to the preservation of liberty" precisely because it "preclude[s] the exercise of arbitrary power" by any one of the three coequal branches of the Federal government. *Mistretta v. United States*, 488 U.S. 361, 380 (1989); *Youngstown*, 343 U.S at 629; *see also Hamdan*, 126 S. Ct. at 2800 ("Concentration of power puts personal liberty in peril of arbitrary action by officials, an incursion the Constitution's three-part system is designed to avoid.") (Kennedy, J., concurring).

In recognition of this deliberate allocation of authority, the Court has long understood that "Presidential powers are not fixed but fluctuate, depending upon their disjunction or conjunction with those of Congress." *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring). "When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb." *Id.* at 637. National security concerns cannot abrogate this fundamental precept of our system of government.[37]

Congressional limitations on the prerogative of the Executive are particularly apt with respect to common law evidentiary privileges, such as the state secrets privilege. *See Dickerson v. United States*, 530 U.S. 428, 437 (2000) ("Congress retains the ultimate authority to modify or set aside any judicially created rules of evidence and procedure that are not required by the Constitution.") (citation omitted); *United States v. Fell*, 360 F.3d 135, 145 (2d Cir. 2004) (subject only to the Constitution, "Congress has the ability to set forth rules of evidence in federal trial."). As both the Second and Ninth Circuits have recognized, Congress may, through statute, alter the contours of the state secrets privilege. *See Halpern*, 258 F.2d at 43 (holding that the creation of a private cause of action that necessarily implicated secret information waived the privilege); *Kasza*, 133 F.3d at 1167 (where Congress "speaks directly to the question otherwise answered by federal common law"—including procedures for state secrets—the judgment of Congress binds both the Executive and the Courts) (internal citation and alterations omitted); *see also Tenet*, 544 U.S. at 11 (where "the national interest would be well served . . . Congress can modify the federal common-law rule announced in *Totten*") (Stevens, J., concurring). As the next section demonstrates, Congress has directly addressed the procedures for handling confidential information in exactly the present situation; hence its rules must be respected, and no dismissal may occur at the outset, before application of those rules to the evidence at hand.

B. FISA's Well-Defined Procedures Govern Secret Information Relating to Electronic Surveillance.

In 1978, the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known informally as the "Church Committee," concluded "that warrantless electronic surveillance in the name of national security ha[d] been seriously

---

[37] *See Hamdi*, 542 U.S. at 536 (plurality) ("Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake."); *Hamdan*, 126 S. Ct. at 2774 n.23 ("Whether or not the President has independent power, absent Congressional authorization . . . he may not disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers."); *Home Bldg. & Loan Ass'n v. Blaisdell*, 290 U.S. 398, 425-26 (1934) ("Emergency does not increase granted power or remove or diminish the restrictions imposed upon power granted or reserved . . . .").

FENWICK & WEST LLP ATTORNEYS AT LAW SAN FRANCISCO

abused." S. Rep. No. 95-604(I) at 7-8, (1978) *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908. In response, Congress endeavored "to curb the practice by which the executive branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." *Id*. The result of these efforts was the Foreign Intelligence Surveillance Act of 1978, "a precisely drawn legislative charter," S. Rep. No. 94-755(II), at 309 (1976), intended to "regulate the exercise of [presidential] authority" over intelligence surveillance. S. Rep. No. 95-604(I), at 16 (1978) *reprinted in* 1978 U.S.C.C.A.N. 3904, 3916.

With FISA, "Congress, in the proper exercise of its powers as an independent branch of government . . . set limits on the President's authority." *Hamdan*, 126 S. Ct. at 2799 (Kennedy, J., concurring). FISA, like the statutes at issue in *Youngstown* and *Hamdan*, was the result of "a deliberative and reflective process engaging both of the political branches." *Id.*; *see also Youngstown*, 343 U.S. at 660 (Burton, J., concurring) ("The controlling fact here is that Congress, within its constitutionally delegated power, has prescribed for the President specific procedures… for his use in meeting the present type of emergency."). The President, therefore, cannot disregard the limitations that Congress, through FISA, has properly placed on executive power.

By prescribing the "exclusive means by which electronic surveillance . . . and the interception of domestic . . . communications may be conducted," FISA and Title III displaced pre-existing federal laws within their scope. Pub. L. No. 95-511, 92 Stat. 1783, § 201 (1978), codified as amended at 18 U.S.C. § 2511(2)(f). This comprehensive overhaul of the federal law of intelligence surveillance includes a number of private rights of action permitting "aggrieved person[s]" civil recovery. *See* 18 U.S.C. § 2520(a) (civil cause of action for interception of communications in violation of Title III); 50 U.S.C. § 1810(a)(I) (same for electronic surveillance in violation of FISA); 18 U.S.C. § 2707(a) (same for unlawful disclosures by communications providers under SCA); 50 U.S.C. § 1809 (prohibiting "electronic surveillance under color of law except as authorized by statute"); 47 U.S.C. § 605(e)(3)(A) (same for unlawful disclosures by communications providers under Communication Act).

Congress, no doubt, understood when it created these private causes of action that lawsuits involving foreign intelligence surveillance would frequently involve state secrets. Certainly, Congress did not intend to "create[] rights which are completely illusory, existing only at the mercy of government officials." *Halpern*, 258 F.2d at 43. Precisely because it foresaw cases like those now facing this Court, Congress dictated a detailed procedure for courts to follow whenever the Government invokes the state secrets privilege in cases involving electronic surveillance. *See* 50 U.S.C. § 1806(f).

The five-step protocol outlined in § 1806(f) is as follows:

1. The court must await a "motion or request . . . by an aggrieved person . . . to discover or obtain . . . materials relating to electronic surveillance." 50 U.S.C. § 1806(f).

2. Following such a request, "the Attorney General [may] file[] an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States." *Id.*

3. Upon receipt of that affidavit, the "court . . . shall . . . review in camera and *ex parte*" any materials about the surveillance "as may be necessary [to allow the court] to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Id.*

4. Based upon that submission, the court decides whether to "disclose to the aggrieved person" any "materials related to the surveillance"—a step that is permissible "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.*

5. Where disclosure to the plaintiff is necessary, the court discloses the materials subject to "appropriate security procedures and protective orders." *Id.*

This procedure applies, without qualification and "notwithstanding any other law," to discovery of any materials relating to "electronic surveillance," a term defined to encompass any "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication . . . without the consent of any party thereto." *Id.*; 50 U.S.C. § 1801(f)(2); *see also* S. Rep. No. 95-604(I), at 57 (1978*) reprinted in* 1978 U.S.C.C.A.N. 3904, 3958 (procedures "apply whatever the underlying rule or statute referred to in [a party's] motion"). This protocol applies to claims in state or federal court, based on state as well as federal law. *Id. See also Riordan* Remand Order, 483 F. Supp. 2d at 940 (finding § 1806(f) "contemplate[s] state court litigation"). Likewise, it governs discovery not only of Verizon's and MCI's disclosures of communications content, but their divulgence of call records as well. 50 U.S.C. § 1806(f) (applies to efforts to "discover or obtain . . . materials *relating to* electronic surveillance") (emphasis added); 50 U.S.C. § 1801(f)(1) (defining "electronic surveillance" to include acquisition of "contents of any wire or radio communication"); 50 U.S.C. § 1801(n) (defining "contents" to include "any information concerning the *identity of the parties* to such communication or the *existence* . . . of that communication.") (emphasis added).

The procedures outlined in § 1806(f) apply regardless of whether the Government has acknowledged the challenged surveillance. *Al-Haramain*, 451 F. Supp. 2d at 1231 ("To accept the government's argument that Section 1806(f) is only applicable when the government intends to use information against a party would nullify FISA's private remedy and would be contrary to the plain language of Section 1806(f)."). Not only is the procedure outlined in § 1806(f) applicable, Congress made this protocol the sole means by which the Executive can assert the state secrets privilege over information related to electronic surveillance. When the legality of surveillance is at issue, "it is this procedure 'notwithstanding any other law' that must be used to resolve the question." S. Rep. No. 95-604(I), at 57 (1978) *reprinted in* 1978 U.S.C.C.A.N. 3904, 3958.

C. Dismissal on the Pleadings Is Impermissible Under § 1806(f).

Rather than mandating dismissal as the Government urges here, the five-step protocol established by Congress provides Plaintiffs with an opportunity to seek redress while guarding against unnecessary disclosures of secret information. Section 1806(f) requires the court not to dismiss claims involving secret surveillance information, but to review the secret material in order to decide "whether the surveillance of the aggrieved person was lawfully authorized and conducted" and, if necessary, disclose the material to the aggrieved party under appropriate security procedures. *Id.*; *ACLU Found. of Southern Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991). Because it contains no reference whatsoever to dismissal, on the pleadings or otherwise, § 1806(f) serves as an unambiguous rejection of such premature termination of litigation in the electronic surveillance context.

Where, as here, Congress has enacted legislation that evinces its "intent to replace the government's evidentiary privilege to withhold sensitive information" with a different protocol, the common law rules must yield to legislative constraints. *Kasza*, 133 F.3d at 1168. The Government cannot simply ignore limitations that Congress has, in proper exercise of its own authority, placed on the Executive's powers. *See, e.g.*, *Hamdan*, 126 S. Ct. at 2774 n.23; *Youngstown*, 343 U.S. at 645-46 (Jackson, J., concurring) (stating that the President's "command power . . . is subject to limitations consistent with a constitutional Republic whose law and policy-making branch is a representative Congress"). The Executive's interest in maintaining secrecy, regardless of its strength, must yield to the reasoned enactments of Congress. *See id.* By crafting an explicit statutory procedure for the invocation and adjudication of the state secrets privilege in the context of electronic surveillance, Congress has left the Executive devoid of authority to assert the privilege as, in essence, an immunity requiring dismissal of these actions.

In short, Congress may not only draw the line between personal liberty and national security, as it has in enacting FISA and the other statutes at issue; it may lay down a specific procedure for courts to employ to determine whether that line has been crossed. With FISA, Congress did just that.

FENWICK & WEST LLP
ATTORNEYS AT LAW
SAN FRANCISCO

CONCLUSION

For the reasons set forth above, this Court should deny the Motion to Dismiss or For Summary Judgment by the United States, and should deny Verizon's Motions to Dismiss insofar as they rely upon the state secrets privilege or related doctrines.

Dated: June 22, 2007

Respectfully,

FENWICK & WEST LLP

By: /s/ Laurence F. Pulgram
Laurence F. Pulgram

Attorneys for Plaintiffs
Dennis P. Riordan, *et al.*

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA

By: /s/ Ann Brick
Ann Brick

Attorneys for Plaintiffs
Dennis P. Riordan, *et al.*

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP

By: /s/ Barry R. Himmelstein
Barry R. Himmelstein

Interim Class Counsel for MCI Class

MOTLEY RICE LLC

By: /s/ Vincent I. Parrett
Vincent I. Parrett

Interim Class Counsel for Verizon Class

GRIFFIN WHITAKER LLP

By: /s/ Joshua Graeme Whitaker
Joshua Graeme Whitaker

Attorneys for Plaintiffs
Christopher Bready, *et al.*

SHAPIRO & STERNLIEB, LLC

By: /s/ David H. Sternlieb
David H. Sternlieb

Attorneys for Plaintiffs
Glen Chulsky, *et al.*

Pursuant to General Order 45, Part X-B, the filer attests that concurrence in the filing of this document has been obtained from Laurence F. Pulgram, Ann Brick, Barry R. Himmelstein, Vincent I. Parrett, Joshua Graeme Whitaker, and David H. Sternlieb.